

## **GeneOS 3.0.0 Provisioning Guide**

GeneOS 3.0.0 Provisioning Guide Rev. A

GENDOC-GENEOS-300-PG. Published on December 6, 2016.

Copyright and Legal Notice

Copyright © 2016 Genexis B.V. All rights reserved.

Genexis B.V., Genexis Holding B.V. and its subsidiaries herein collectively known as Genexis.

GeneOS, programme models and other software content and this documentation ("the Intellectual Property Rights") are protected by the Dutch Copyright Act ('Auteurswet') and Genexis declares that it is the author and claims copyright ('Auteursrecht') for the Intellectual Property Rights. Reproduction and distribution without authorisation by Genexis B.V. is prohibited. The prohibition includes every form of reproduction and distribution.

Every effort has been made to ensure that the information in this document is complete and accurate at the time of printing. However, information is subject to change without notice. Genexis assumes no liability for damages incurred directly or indirectly from errors, omissions or discrepancies between the software and this document.

Genexis, FiberXport and DRG are trademarks of Genexis.

All other trademarks, service marks and trade names are the property of their respective owners. Purchasers, licensees and users accept and acknowledge that the products contain components (including components carrying certain firmware) and combinations of components that constitute trade secrets protected by Genexis or its partners. Purchasers, licensees and users warrant that the delivered products will not be opened or dismantled, copied, altered or in any other way modified. Furthermore, purchasers, licensees and users agree not to attempt to reverse engineer, disassemble, modify, translate, create derivative works, rent, lease, loan, or without written permission distribute or sublicense the software, in whole or in part.

The products and its hardware, firmware and software, including technical data, may be subject to EU and U.S. export control laws, including the U.S. Export Administration Act and its associated regulations and the International Traffic in Arms Regulations administered by the US Department of State, and may be subject to export or import regulations in other countries. Purchasers and licensees agree to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import hardware, firmware and software.

Purchasers and licensees are not entitled to, and Genexis is not in any event liable to pay compensation for damages which delivered products or software has caused to other property or to persons or any other consequential damages, including but not limited to loss of profit, loss of production or any other indirect damages.

# Contents

---

<b>Introduction</b>	<b>1</b>
Configuration Strategy (Bootstrapping the CPE)	1
Method Overview	2
CLI (Command Line Interface)	2
CWMP (CPE WAN Management Protocol)	2
DHCP	2
GAPS	2
GUI	2
Supported Platforms	3
Related Documents	4
Typographical Conventions	5
Symbols Used	6
 <b>CLI Management</b>	 <b>7</b>
Connecting	7
Command structure	7
Fast text entry	9
Getting help	10
Command history and editing	11
Keyboard shortcuts	11
Tasks	12
Checking product information	12
Changing the default password	12
Changing the hostname	12
Setting the date and time	13
Configure System Logging	14
Viewing current (active) configuration	16
Saving the current configuration	16
Upgrading firmware	16
Upgrading the bootloader	16
Rebooting	17
Configuring the Management Interface	17

<b>CWMP Management</b>	<b>20</b>
TR-069 Protocol and Data Models	20
Partial Profile Support	22
Vendor extensions	23
Connecting	31
ACS Discovery	31
CPE Behaviour	31
Manual Configuration	32
Tasks	33
Checking product information	33
Changing the default password	33
Changing the hostname	33
Setting the date and time	33
Configure System Logging	33
Viewing current (active) configuration	33
Saving the current configuration	33
Upgrading firmware or bootloader	34
Rebooting	34
Configuring the Management Interface	34
<b>DHCP</b>	<b>35</b>
Connecting	35
DHCP Request Process	35
Assigning a Static IP to a CPE	38
DHCP Server Response	39
Using DHCP for ACS Discovery	39
Option 43 (Vendor Specific Information)	39
Option 125 (Vendor Identifying Vendor Specific Information)	41
Tasks	44
Checking product information	44
Changing the hostname	44
Other tasks	44
<b>Appendix A. DHCP Client ID</b>	<b>45</b>
Type	45
IAID (Interface Association Identifier)	46
DUID (DHCP Unique Identifier)	47
<b>Appendix B. DHCP for Windows</b>	<b>48</b>
Creating a Reservation (static mapping)	48
Sending Vendor Specific Options	51
Option 43	52
Troubleshooting	60
Option 125	61
Troubleshooting	71
<b>Appendix C. Glossary</b>	<b>72</b>

# List of Tables

---

Supported platforms and models .....	3
File name release types .....	3
Related documents .....	4
CLI keyboard shortcuts .....	11
Logging message severity levels .....	14
User:1 Profile Support .....	22
Time:1 Profile Support .....	22
Management Interface TR-069 Vendor Extensions .....	23
Hostname TR-069 Vendor Extensions .....	23
Firewall - ICMP TR-069 Vendor Extensions .....	23
DHCPv4 Client TR-069 Vendor Extensions .....	24
Ethernet.Link TR-069 Vendor Extensions .....	25
System Logging TR-069 Vendor Extensions .....	26
Device.Time TR-069 Vendor Extensions .....	27
CATV TR-069 Vendor Extensions .....	28
IGMP TR-069 Vendor Extensions .....	29
Parameters for upgrading via CWMP .....	34
Options included in DHCP client request .....	35
Required DHCP Options .....	36
Optional DHCP Options .....	36
Broadband Forum Option 43 codes .....	39
Broadband Forum Option 125 codes .....	41
Vendor ID for encapsulating ACS parameters .....	41
IAID bit fields .....	46
DUID byte fields .....	47
Data for option 43 .....	52
Data for option 125 .....	62

# Introduction

---

GeneOS is the firmware installed on Genexis Customer Premises Equipment (CPEs). GeneOS provides several methods with which CPEs can be configured and managed.

The purpose of this manual is to provide an overview of each configuration method and to describe how to connect to and interact with the CPE using each method.

Each chapter covers one specific configuration method, describing how to perform an initial configuration of the CPE in preparation for connecting it to a management network. This includes setting basic parameters such as the hostname and configuring the management interface.

Also shown are basic maintenance commands such as how to upgrade firmware and reboot the CPE.



**Warning:** Attempting to configure the device using multiple methods (such as both CLI and CWMP) simultaneously may result in unexpected behaviour.

---

Guidelines for configuring the CPE for integration into specific deployment scenarios can be found in the **GENEOS SERVICE CONFIGURATION GUIDE**.

## Configuration Strategy (Bootstrapping the CPE)

CPE management is done via the WAN (upstream) interface. By default, this interface is a member of VLAN 1 (untagged) and is used as the source interface for all management, CWMP and VoIP traffic.

The recommended approach for configuring the CPE is to connect to its management interface and provide the CPE with enough information (such as VLAN settings) to enable it to connect to a management network. Once connected, full configuration can be completed.



**Stop:** All operators **must** change the password for the user 'operator'. Failure to do so renders the device accessible to anyone who knows the default password. Changing the password can be done via the CLI or CWMP.

---



**Warning:** It is important to understand that the instructions in this document are only for configuring the CPE itself. This document does not cover how to enable and configure the various services the CPE supports, such as Internet and VoIP. For that, please refer to the document **GENEOS SERVICE CONFIGURATION GUIDE**

---

## Method Overview

### CLI (Command Line Interface)

The network operator accesses the command line interface (CLI) via remote SSH connection. Configuration is done manually by typing in a series of commands. Please see the CLI chapter on page 7.

A detailed description of all commands and their syntax is available in the [GENEOS COMMAND LINE REFERENCE](#).

### CWMP (CPE WAN Management Protocol)

The operator can configure and monitor CPEs from an Auto Configuration Server (ACS). Communication between the CPE and the ACS complies with CWMP as defined by TR-069.

The CPE supports a combination of TR-069, TR-104 and TR-181 standard profiles and vendor extended profiles. Please see the chapter on CWMP Management on page 20.

### DHCP

A DHCP server can be used to not only provide the CPE's management interface with an IP address, but to deliver supplemental information such as ACS server. The DHCP chapter on page 35 explains this in full.

### GAPS

The Genexis Automatic Provisioning System is a central office solution for remotely managing Genexis CPEs.

As of GeneOS 2.3.0, commands are available for configuring certain aspects of the CPE's interactions with GAPS. However, until GAPS is released these commands do not have any effect, nor are they documented.

A new version of the GeneOS documentation will be released in conjunction with GAPS in which these commands are included.

### GUI

End users can make use of a web-based GUI to configure certain features of their CPE.

## Supported Platforms

GeneOS supports multiple products that can be grouped logically into software platforms. GeneOS firmware releases include images for each supported platform. The firmware image name includes the platform name, version number and the release type in the following format:

*geneos-<platform>-<version>-<release type>.img*

For example, *geneos-lunar-3.0.0-R.img* indicates a full release of GeneOS version 3.0.0 for the Lunar platform.

A CPE's platform can be determined from information provided by the device itself. Instructions for doing so are included for each management method in its respective chapter in the [GENEOS PROVISIONING GUIDE](#).

Platform	Model	Architecture
Lunar	Platinum-7840 DRG 78x0	Lunar devices operate at Layer 3, routing traffic from the user's LAN.
Polar	FiberTwist-P2410	Polar devices operate at Layer 2, bridging traffic from the user's LAN.

Table 1. Supported platforms and models

The following table lists each release type and the associate code used in the <release type> section of the filename.

Code	Meaning	Description
R	Full release	Full release for all supported platforms. Includes complete documentation and release notes.
RC	Release candidate	Full release that may be limited in some way (e.g. to a particular platform). May not include all documentation.
EFT	Early Field Trial	Early release made available to a limited number of customers. Used to provide a hot fix or demonstrate a new feature.

Table 2. File name release types



## Related Documents

This document is meant to be read in conjunction with the following additional resources.

Document	Content
GENEOS COMMAND LINE REFERENCE	A list of all CLI commands and their full syntax.
GENEOS RELEASE NOTES	When a new version of GeneOS is released, this document describes new features, resolved problems and issues still being worked on.
GENEOS SERVICE CONFIGURATION GUIDE	Instructions for implementing specific deployment scenarios and use cases using the CLI.
GENEOS GUI USER GUIDE	Brief introduction to connecting to and using the Graphical User Interface.

Table 3. Related documents

## Typographical Conventions

- Fixed width font indicates sample output:

```
Genexis Operating System (GeneOS)
Copyright (c) 2009-2016 Genexis B.V. All rights reserved.
GeneOS version: geneos-lunar-3.0.0-R
geneos#
```

- **Bold text** in sample output indicates a command the user has to type in order for the output shown to be generated:

```
geneos# show version
Genexis Operating System (GeneOS)
Copyright (c) 2009-2016 Genexis B.V. All rights reserved.

GeneOS version: geneos-lunar-3.0.0-R
Compiled: Mon Oct 19 10:51:59 CEST 2015
```

- **<text in angled brackets>** in a command indicates a parameter that the user needs to change to the correct value for their system. For example a command given as

```
geneos# copy <source-URL> <destination>
```

should be typed in and executed with genuine URLs such as

```
geneos# copy tftp://example.com/source.img bootflash
```

- **[text in square brackets]** in a command indicate an optional parameter. It only needs to be included if relevant.
- *Italics* indicate a filename:  
*geneos-polar-3.0.0-R.img*
- **<TAB>** regular text in angled brackets indicates a keyboard key to be pressed.

## Symbols Used

The following symbols are used in this document to bring attention to certain details.



**Note:** Anything included as a note is there to provide supplemental information or to clarify a particular topic.

---



**Tip:** It is not necessary to do this, but it may help make things easier or more efficient.

---



**Warning:** Understand the text and its implications before implementing or choosing not to implement a particular feature or follow a specific instruction.

---



**Stop:** Failure to understand the text or follow the instruction could result in a loss of information, device inoperability, unreliable or unexpected behaviour.

---

# CLI Management

---

The command line interface (CLI) is used to configure and manage Genexis GeneOS CPEs. All changes to the CPE's configuration are automatically saved.

For a complete reference to all CLI commands and their syntax, consult the [GENEOS COMMAND LINE REFERENCE](#).

## Connecting

Accessing the CLI is done by establishing an SSH connection. On Mac OS X and Linux based systems this can be done via the traditional Terminal application. Windows users will need to download and install an SSH client such as PuTTY (<http://www.putty.org>).

The default username/password is **operator/operator**.

```
$ ssh operator@192.168.42.1>
operator@192.168.42.1's password: operator
Genexis Operating System (GeneOS)
Copyright (c) 2009-2016 Genexis B.V. All rights reserved.
GeneOS version: geneos-lunar-3.0.0-R
geneos#
```

Once the SSH connection is established, the CPE is configured by typing the appropriate commands at the prompt.

## Command structure

The set of commands exists in a hierarchy. The commands available at any given point depend on the user mode and the user's location with the hierarchy. Both the mode and current location in the hierarchy are indicated by the prompt. The prompt also reflects the hostname of the device.

```
geneos#
geneos(config)#
geneos(config-if-wan)#

CPE-42#
CPE-42(config)#
```

The first line shows the default prompt and indicates the device is in **admin mode**.

The prompt on the second line shows the device is now in **configuration mode**.

On the third line, the prompt reflects that the user has moved further down the command hierarchy into WAN interface configuration context.

The last two lines show the user has changed the hostname of the device to CPE-42.

```
geneos# configure terminal  
geneos(config)#
```

Entering **configure terminal** at the default prompt puts the user in **configuration mode**. This change of mode is reflected in the new prompt.

```
geneos(config)# interface wan  
geneos(config-if-wan)#
```

Once in configuration mode, it is possible to move through the command hierarchy. **interface wan** for example puts the user in WAN interface configuration context and the prompt changes to reflect this.

```
geneos(config-if-wan)# exit  
geneos(config)#
```

To move back up a single level in the hierarchy, enter **exit**.

```
geneos(config-if-wan)# end  
geneos#  
  
geneos(config-if-wan)# ^c  
geneos#
```

To move directly to admin mode from anywhere in the hierarchy, enter **end**.  
Typing **ctrl-c** is an alternative to typing **end**.

```
geneos(config-if-wan)# do show running-config  
! version geneos-lunar-3.0.0-R  
geneos(config-if-wan)#
```

It is not necessary to move through the hierarchy in order to execute admin level commands. By utilising the **do** command, admin level commands can be run without having to leave the current position in the hierarchy.

```
geneos# quit  
geneos# Connection to 192.168.42.1 closed.  
$
```

The **quit** command (available in admin mode) logs the current user out and closes the connection.

## Fast text entry

There are two mechanisms in place to allow faster and more efficient text entry.

### Tab completion

The <TAB> key auto-completes the current command. Type the initial characters of a command and then hit <TAB>. A list of available commands matching that string will be displayed (see lines 1-3).

If there is only one match, the full command is typed out automatically as shown on the last line.

```
geneos# co<TAB>
  configure  Enter configuration mode
  copy       Copy from one file to another
geneos#

geneos# sho<TAB>
geneos# show
```

### Abbreviated command entry

Rather than typing out each command in full, it is only necessary to type enough of the command's initial letters for the system to uniquely identify it.

```
geneos# s v
Genexis Operating System (GeneOS)
Copyright (c) 2009-2016 Genexis B.V. All rights reserved.

geneos# co
%-ERR: co
      ^^ Ambiguous command
geneos#
```

On line 1, **show** is the only command that starts with an "s" and **version** the only option beginning with a "v". There is no ambiguity in this command and it therefore executed successfully.

In the second example, "co" contained insufficient initial letters to differentiate the command. "co" could either be **copy** or **configure**. This ambiguity is reflected in the error message.

## Getting help

Context sensitive help is available at any time by entering a question mark <?>

```
geneos# co?  
  configure  Enter configuration mode  
  copy       Copy from one file to another  
geneos# co
```

A question mark with *no* space before it lists all the commands or options that start with those letters.

```
geneos# show ?  
  clock      Show system clock  
  cwmpp      Show CWMP information  
  history    Show command line history  
  interface  Interface information  
  logging    Log messages  
  running-config Show running configuration  
  tech-support Show information for Technical Support  
  version    Show version info  
geneos# show
```

When there *is* a space between the command and the question mark, all possible command options will be displayed.

```
geneos# ?  
  configure  Enter configuration mode  
  copy       Copy from one file to another  
  quit       Exit shell  
  reload     Reload system  
  show       Show running system information  
  write      Write running configuration  
  <cr>       (Executes '')  
geneos#
```

If entered alone as illustrated above, the question mark lists all available commands.

## Command history and editing

Once entered, commands are stored in a history buffer. This buffer can be accessed via the up and down arrow keys. The buffer is maintained only for the lifetime of a session.

Once a command has been entered, either by typing it in directly or finding it in the command history, it is possible to edit it before execution. The following section lists all the possible editing methods and their shortcuts.



**Tip:** instead of always typing the shortest possible command it can be useful to type enough letters to make it recognisable when it appears in the history list. For example, enter **sh ver** instead of **s v** for "show version".

## Keyboard shortcuts

Keyboard shortcuts are available for cursor placement, text editing, accessing help and navigating history.

Key		Function
<Enter>		Execute the command
Ctrl-A		Move cursor to the start of the line
Ctrl-E		Move the cursor to the end of the line
Ctrl-C		Abort the command or exit out of configuration mode and back into admin mode
Ctrl-K		Delete all characters from the right of the cursor to the end of the line
Ctrl-U	Ctrl-W	Delete all characters from the left of the cursor to the start of the line
Ctrl-L		Redraw the last line (after having been overwritten)
↓ (down arrow)	Ctrl-N	Move down the history list
↑ (up arrow)	Ctrl-P	Move up the history list
→ (right arrow)	Ctrl-F	Move cursor to the right
← (left arrow)	Ctrl-B	Move cursor to the left
⌫ (backspace)		Delete the character to the left of the cursor
⌫ (delete)	Ctrl-D	Delete the character to the right of the cursor
→ (TAB)		Expand the command or display options (see "Getting Help")
? (question mark)		Show list of available commands or display options (see "Getting Help")

Table 4. CLI keyboard shortcuts



## Tasks

### Checking product information

**show version** displays information such as firmware platform and version, the product name and MAC address.

```
geneos# show version
Genexis Operating System (GeneOS)
Copyright (c) 2009-2016 Genexis B.V. All rights reserved.

GeneOS version: geneos-lunar-3.0.0-R
Compiled: Mon May 19 10:51:59 CEST 2016
Source ID: 5054502a17e5542740c978d4a7d0a7116507fcd4
          72c691f1d6ce7be49402d5a4d534d65abfe80646

Uptime is 4h39m19s
Last boot: unknown

Bootloader version: bootloader-lunar-3.0.0-R
Bootstrap version: bootstrap-lunar-3.0.0-R

Product name: Platinum-7840
Product number: 99110000
Product revision: 0.2
Product date: 2016-01-01
Serial number: W.0000000042
Base MAC address: 000F94000000
geneos#
```

### Changing the default password

Enter configuration mode and use the **username** command to change the password for the “operator” user.

```
geneos# configure terminal
geneos(config)# username operator password <newpassword>
geneos(config)#
```

### Changing the hostname

The hostname can be changed in configuration mode. The change will not be reflected in the prompt until the user exits back to admin mode.

```
geneos# configure terminal
geneos(config)# hostname <CPE-42>
geneos(config)# exit
CPE-42#
```

## Setting the date and time

There are two configuration mode commands that work together to set and display the correct date and time.

1. **ntp server** - to specify an ntp server to which the CPE will synchronise its clock
2. **clock timezone** - for displaying the date and time in the local timezone

```
geneos# configure terminal
geneos(config)# ntp server <pool.ntp.org>
geneos(config)# ntp server <195.43.138.123>
geneos(config)# clock timezone <Europe/Luxembourg>
geneos(config)# do show clock
Mon Aug 22 15:05:45 2016 UTC
```

**ntp server** is used to specify up to 5 individual ntp servers. The servers can be specified as either hostnames or IP addresses.

As shown above, by default the CPE displays the date and time information as UTC time. This can be changed with the **clock timezone** command.

Timezone information is set using Olsen format. In this format, timezones are specified as Area/Location pairs. For a full list of Area/Location combinations supported by GeneOS, use the ? help command to list them. The output below is a small sample of all available timezones.

```
geneos(config)# clock timezone ?
Africa/Cairo
Africa/Casablanca
Africa/Johannesburg
America/Anchorage
America/Chicago
America/El_Salvador
America/Halifax
Antarctica/Davis
Asia/Baghdad
Asia/Damascus
Australia/ACT
Australia/Adelaide
Australia/Broken_Hill
Europe/Amsterdam
Europe/Athens
Europe/Belfast
geneos(config)# clock timezone <Australia/Brisbane>
geneos(config)# do show clock
Mon Aug 23 01:05:46 2016 AEST
```

Once the timezone is set, all date and time information will be displayed using that timezone.

## Viewing the date and time

To view the current date, time and timezone, use the **show clock** command:

```
geneos# show clock
Mon Aug 23 01:05:46 2016 AEST
```

The timezone can also be seen in the output of **show running-config** command:

```
geneos# show running-config
! version geneos-lunar-2.3.0-N160821
clock timezone Australia/Brisbane
```

In rare circumstances, the output of **show running-config** command: may look as follows:

```
geneos# show running-config
! version geneos-lunar-2.3.0-N160821
clock timezone TZ=GRNLNDST3GRNLNDDT,M10.3.0/00:00:00,M2.4.0/00:00:00
```

In the output above, the date and time is shown in POSIX format. This occurs if the timezone has been set via CWMP using POSIX format.

Using the CLI, timezone information can only be set in Olson format.

However, CWMP permits the timezone to be set in either Olsen or POSIX format.

If CWMP is used to set the timezone in POSIX format, the CLI will display it in POSIX format.

## Configure System Logging

During normal operation the various components and subsystems of the CPE generate logging messages.

Each log entry is assigned a severity level (between 0 and 7) for the purpose of differentiating between messages that are merely informational and those which indicate problems.

The following table lists each severity level and its description.

Level	Name	Description
0	emergencies	System is unusable
1	alerts	Immediate action needed
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant conditions
6	informational	Informational messages
7	debugging	Debugging messages

Table 5. Logging message severity levels

The default behaviour is to log all messages locally on the device.

To change this behaviour, two commands are available:

1. **logging server** - to log messages to a remote syslog server
2. **logging console** - to specify the severity levels to log locally on the device.

## logging server

Use this command to specify a remote syslog server to which all logging messages are to be sent.



**Note:** Remote logging always sends messages of **all** severity levels to the remote syslog server. Any required filtering can be done on the remote server.

Set the remote syslog server as follows:

```
geneos# configure terminal
geneos(config)# logging server <192.168.42.227> [port <512>]
geneos(config)#
```

Specifying the port is optional. If no port is specified, it defaults to using UDP port 512. The remote server can be specified as either a hostname or an IP address.

## logging console

Use this command to specify which severity levels are logged locally on the device.

Specifying a severity level means all messages of that level **and lower** are logged. For example, specifying a level of errors (level 3) will log messages of severity: errors (level 3), critical (level 2), alerts (level 1) and emergencies (level 0).

The following commands logs severity level “errors” and lower to the local device:

```
geneos# configure terminal
geneos(config)# logging console errors
geneos(config)#
```

## Testing

It is possible to test logging behaviour with the **test logging** command. Send a test message with this command and then view logged messages with the **show logging** command. Details of syntax are provided in the GENEOS COMMAND LINE REFERENCE.

```
geneos# test logging message debugging “Testing 1 2 3 4”
geneos# show logging level debugging
Nov 17 20:04:25 geneos user.debug operator: Testing 1 2 3 4
geneos#
```

If a remote syslog server has been configured, the test message will also be sent to the remote server. The following output is from a Linux server running syslogd.

```
Nov 17 20:04:25 192.168.42.1 operator: Testing 1 2 3 4
```

## Viewing current (active) configuration

Enter **show running-config** to view the currently active configuration. The output will differ between devices.

An **!** (exclamation mark) indicates a line that reflects the default configuration.

```
geneos# show running-config
! version geneos-lunar-3.0.0-R
!cwmpt acs username "000F94-Lunar-W%2E0000430013" password ""

interface vlan1
  !ip address dhcp

interface wan
  !vlan member 1
  !vlan untagged 1
!end
geneos#
```

## Saving the current configuration

The configuration is automatically saved whenever changes are made.

## Upgrading firmware

Save the new firmware image on either an HTTP or TFTP server that's accessible by the CPE.

Use the **copy** command to download the new firmware from the server to the CPE. Once the download has completed, the new firmware will be installed automatically. Reboot the CPE to make the new firmware active.

```
geneos# copy <http://192.168.42.229/geneos-lunar-2.2.1-R.img> bootflash
Connecting to 192.168.42.229 (192.168.42.229:80)
Download successfully.
Firmware has been successfully upgraded.
geneos# reload
Reboot the system. Are you sure? [y/N]: y
Rebooting system
geneos# Connection to 192.168.42.1 closed by remote host.
$
```

## Upgrading the bootloader

If asked to upgrade the bootloader, save the new image on either an HTTP or TFTP server that's accessible by the CPE.

Use the **copy** command to download the new firmware from the server to the CPE.

```
geneos# copy <tftp://192.168.42.229/bootloader-lunar-3.1.0.img> bootloader
```

The bootloader is downloaded, validated, and written to flash (if valid). The new bootloader will be used when the CPE is rebooted. Use the **show version** command to verify the bootloader version being used.

## Rebooting

The **reload** command available in admin configuration mode reboots the CPE.

```
geneos# reload
Reboot the system. Are you sure? [y/N]: y
Rebooting system
geneos# Connection to 192.168.42.1 closed by remote host.
$
```

## Configuring the Management Interface

This a three step process:

1. The WAN interface needs to be made a member of the appropriate VLAN(s).
2. The VLAN(s) need to be configured with appropriate layer 3 settings such IP address and access list membership.
3. Specify over which VLAN management traffic is to be transported.

The default (factory) configuration for the WAN interface (shown below) makes it an untagged member of VLAN 1, receiving an IP address from a DHCP server. All management traffic is sent over VLAN 1.

```
!management source-interface vlan1

interface vlan1
!ip address dhcp

interface wan
!vlan member 1
!vlan untagged 1
```

### 1. Modify the VLAN membership of the WAN interface.

Use the **vlan** command as shown below.

```
geneos# configure terminal
geneos(config)# interface wan
geneos(config-if-wan)# vlan member <42,100,200-210>
geneos(config-if-wan)# vlan untagged <42>
```

The above set of commands makes the WAN interface a member of VLANs 42, 100 and from 200 to 210 inclusive. Traffic through VLAN 42 will be untagged.



**Warning:** When entering a comma separated list of VLANs there should be no space between the comma and the next number. Doing so will result in the following error message:

```
%-ERR: vlan member 42, 100, 200-210
^^^^ Invalid command
```

## 2. Configure the layer 3 properties

In this example, the management network is configured on VLAN 42. It is this interface on which layer 3 properties need to be set.

At the end of step 1, the CPE was in WAN interface context (as evident by the prompt). Jump straight from WAN interface context to VLAN configuration context by using the **interface** command.

```
geneos(config-if-wan)# interface <vlan42>
geneos(config-if-vlan)# ip address dhcp
```

When new interfaces are created, for security reasons all traffic is blocked by default. It is therefore necessary to create an Access Control List to permit relevant traffic on the new interface. This topic is covered in full in the GENEOS SERVICE CONFIGURATION GUIDE, but the example below shows how to permit SSH, DHCP and CWMP connections on the new management VLAN.

In the example below, the network address **192.168.42.0/24** is used to represent an operator's management network. The individual host addresses (for example **192.168.42.239**) show that traffic is restricted to originating from one specific host.

```
geneos# configure terminal
geneos(config)# ip access-list <Management-IN>
geneos(config-acl)# permit tcp source <192.168.42.0/24> destination any port 22
geneos(config-acl)# permit tcp source host <192.168.42.239> destination any port 8082
geneos(config-acl)# permit udp source <192.168.42.0/24> port 68 destination any port 67
geneos(config-acl)# exit
geneos(config)# interface <vlan42>
geneos(config-if-vlan)# ip access-group <Management-IN> in
geneos(config-if-vlan)#
```



**Warning:** Changes made to an interface's IP address and VLAN membership take effect immediately. Care must therefore be taken not to lose access to the CPE. As a last resort, perform a factory reset to regain access.

### 3. Specify the VLAN for management traffic:

At the end of the previous step, the CPE was in VLAN configuration context. The first line of the example below moves up the hierarchy to where the management command is found.

```
geneos(config-if-vlan)# exit
geneos(config)# management source-interface <vlan42>
```

### Result

After following the previous three steps, the completed management interface configuration is as follows:

```
management source-interface vlan42

interface vlan42
!ip address dhcp

interface wan
vlan member 42,100,200-210
vlan untagged 42
```



# CWMP Management

---

The CPE WAN Management Protocol (CWMP) supports remote configuration of GeneOS as defined in TR-069. Configuration is performed using an Auto-Configuration Server (ACS) to set parameters defined in different TR-069 data models.

No special measures are necessary to enable connectivity between the CPE and the ACS. This allows default firewall policies to remain unchanged. The ACS is only allowed to request contact from the CPE using a Connection Request. The CPE only accepts configurations from preconfigured ACS for connections initiated by the CPE itself.

The CPE normally initiates connections to the ACS at configured time intervals, during a boot operation, or if triggered by special events. These connections are used by the ACS to acquire the status of the CPE or to perform configuration changes, firmware upgrades or other tasks.



**Warning:** For some CWMP operations to function correctly, the CPE must be able to synchronise its internal clock to an NTP server. NTP servers can be configured either via the command line or CWMP. Ensure there are no firewall rules or other access controls blocking access to NTP servers on UDP port 123 from the management interface.

## TR-069 Protocol and Data Models

Support for TR-069 in GeneOS includes:

- Remote Procedure Call (RPC) methods as defined in TR-069 Amendment 5 ([https://www.broadband-forum.org/technical/download/TR-069\\_Amendment-5.pdf](https://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf)).
  - Generic Methods:
    - GetRPCMethods
  - CPE Methods:
    - SetParameterValues
    - GetParameterValues
    - GetParameterNames
    - SetParameterAttributes
    - GetParameterAttributes
    - AddObject
    - DeleteObject
    - Download
    - Reboot
    - FactoryReset
    - ScheduleDownload
  - ACS Methods:
    - Inform
    - TransferComplete
    - AutonomousTransferComplete

- Internet Gateway Device Data Model as defined in TR-181 issue 2 Amendment 9 (<https://www.broadband-forum.org/cwmp/tr-181-2-9-0.html>).

If a profile is listed as being partially supported, some objects or parameters in that profile are not yet implemented.

If the partial support is due to the way in which particular parameters are implemented, the differences between the official profile definition and the GeneOS implementation are detailed in the “Partial Profile Support” section on page 22.

- Device:2.0 Profile Definitions
  - AdvancedFirewall:1 (partial)
  - Baseline:3
  - Bridge:1
  - DHCPv4Client:1
  - DHCPv4Server:1
  - DHCPv6Client:1 (partial)
  - DNSRelay:1
  - EthernetInterface:1
  - EthernetLink:1
  - IPInterface:1
  - IPPing:1
  - IPv6Interface:1 (partial)
  - NAT:1 (partial)
  - QoS:1 (partial)
  - Routing:1 (partial)
  - Time:1 (partial implementation - for details see “Table 7. Time:1 Profile Support” on page 22)
  - User:1 (partial implementation - for details, see “Table 6. User:1 Profile Support” on page 22)
  - VLANBridge:1
  - VLANTermination:1
  - WiFiAccessPoint:1 (partial)
  - WiFiRadio:1 (partial)
  - WiFiSSID:1 (partial)

- Provisioning Parameters for VoIP CPE as defined in TR-104i1 (<https://www.broadband-forum.org/cwmp/tr-104-1-1-0.html>).
  - VoiceService:1 Profile Definitions
  - Endpoint:1
  - SIPEndPoint:1

- Vendor Extensions
  - Genexis provides support for GeneOS features via Vendor Extensions.

To retrieve the list of Genexis extensions, use the GetParameterNames RPC method or refer to “Vendor extensions” section on page 23.

## Partial Profile Support

The following tables show for each partially supported profile the level of support **where it differs** from the official profile definition.

### User:1

(<https://www.broadband-forum.org/cwmp/tr-181-2-9-0.html#H.Device:2.User:1>  
Profile)

Name	Capability
Device.Users.User.{i}	Read Only Table (users cannot be added or removed).
Enable	Not supported.
Username	Read Only. The username cannot be changed.
Password	<p>Extended password support:</p> <p>The TR-181 definition implies that passwords are written and stored as clear text values. This is insecure, therefore Genexis has extended this functionality in two ways:</p> <p>Passwords are stored in encrypted format (by default SHA-512).</p> <p>Passwords may be written as encrypted or clear text values.</p> <p>Encrypted values should follow the format of the UNIX cryptpw() function: “\$&lt;method&gt;\$&lt;salt&gt;\$&lt;encrypted password&gt;”.</p> <p>The user’s password may thus be written either as a clear text password of type string(64) per the TR-181 definition or as an encrypted value of type string(128) using one of MD5, SHA-256 or SHA-512 encodings.</p> <p>Passwords provided in clear text will be encrypted using cryptpw() with an SHA-512 hash. Passwords values which are not recognised as cryptpw() values will be treated as clear text.</p> <p>Genexis recommends the use of strong encryption of users’ passwords - SHA-512 is the strongest hash supported.</p>

Table 6. User:1 Profile Support

### Time:1

([https://www.broadband-forum.org/cwmp/tr-181-2-9-0.html#D.Device:2.Device.](https://www.broadband-forum.org/cwmp/tr-181-2-9-0.html#D.Device:2.Device.Time.)  
Time.)

Name	Capability
Status	<p>Only two states are supported:</p> <ul style="list-style-type: none"><li>• Disabled</li><li>• Synchronized</li></ul>

Table 7. Time:1 Profile Support

## Vendor extensions

### Management Interface

Defines the interface that is to be used for management service traffic.

Name	Type	Write	Description	Default
Device. ManagementServer.	object	-		-
X_GENEXIS_EU_ ManagementInterface	string(256)	W	The value MUST be the path name of a row in the IP.Interface table. The value points to the interface over which the management traffic is to be sent. Example: Device.IP.Interface.1	If an empty string is specified, the CPE MUST use the default interface if this exists, or if not as directed by its routing policy to determine the appropriate interface.

Table 8. Management Interface TR-069 Vendor Extensions

### Hostname

Adds the ability to define a name for the device. This can be used by upstream DHCP servers to provide a specific configuration or to uniquely identify the device.

Name	Type	Write	Description	Default
Device. DeviceInfo.	object	-	This object contains the general device information.	-
X_GENEXIS_EU_ Hostname	string(64)	W	The value shall be a valid hostname consistent with RFC1123.	-

Table 9. Hostname TR-069 Vendor Extensions

### Firewall - ICMP support

Provides the ability to define rules as to how to process ICMP messages.

Name	Type	Write	Description	Default
Device. Firewall.Chain.{i}.Rule. {i}.	object	W	This object contains the firewall information.	-
X_GENEXIS_EU_ IcmpType	string	W	The type of ICMP message. Enumeration of: Echo Echo-reply Unreachable	-

Table 10. Firewall - ICMP TR-069 Vendor Extensions

## DHCPv4 Client

Adds capabilities to view additional information supplied by the upstream DHCP server in the device's DHCP lease.

Name	Type	Write	Description	Default
Device.DHCPv4.Client. {i}.	object	W	This object contains DHCP client settings for an associated IP Interface indicated by Interface.	-
X_GENEXIS_EU_ RenewTime	int[-1:]	-	Number of seconds remaining until DHCP lease renew time. A value of -1 indicates this was not specified by the server	-
X_GENEXIS_EU_ RebindTime	int[-1:]	-	Number of seconds remaining until DHCP lease renew time. A value of -1 indicates this was not specified by the server	-
X_GENEXIS_EU_ NextServer	IPAddress(15)	-	The IPv4 address of the next server option provided by the server	-
X_GENEXIS_EU_ Mac	MACAddress	-	The MAC address of the DHCPv4 client.	-
X_GENEXIS_EU_ File	string(256)	-	The URL or filename provide in the bootfile option.	-
X_GENEXIS_EU_ ClientID	string(256)	-	The client identifier of this DHCPv4 client	-
X_GENEXIS_EU_ VendorClassID	string(256)	-	The vendor class identifier of this DHCPv4 client	-

Table 11. DHCPv4 Client TR-069 Vendor Extensions

## Ethernet.Link

Adds the ability to retrieve GeneOS specific identifiers used in with virtual links.

Name	Type	Write	Description	Default
Device.Ethernet.Link.{}	object	–	<p>The Ethernet link layer table (a stackable interface object as described in [Section 4.2/TR-181i2]). Table entries model the Logical Link Control (LLC) layer. It is expected that an Ethernet Link interface can be stacked above any lower-layer interface object capable of carrying Ethernet frames.</p> <p>At most one entry in this table (regardless of whether or not it is enabled) can exist with a given value for Alias, or with a given value for Name. On creation of a new table entry, the CPE MUST choose initial values for Alias and Name such that the new entry does not conflict with any existing entries.</p> <p>At most one enabled entry in this table can exist with a given value for MACAddress.</p>	–
X_GENEXIS_EU_LinkID	string	W	<p>The virtual link identifier. Enumeration of:</p> <ul style="list-style-type: none"> <li>wan</li> <li>wan1</li> <li>wan2</li> <li>wan3</li> <li>wan4</li> <li>lan</li> </ul> <p>Provides information for identification of the specific virtual interface represented by this Ethernet.Link object.</p>	–

Table 12. Ethernet.Link TR-069 Vendor Extensions

## System Logging

This object provides the ability to configure what information the CPE logs and to where it logs it.

Name	Type	Write	Description	Default
Device.X_GENEXIS_EU_Ext.Logging.	object	-	This object contains the Genexis vendor specific logging controls.	-
RemoteServerEnable	boolean	W	Remote server logging enable.	false
RemoteServer	string(256)	W	Hostname or IP address of the remote syslog server for the CPE to send syslog messages if RemoteServerEnable is enabled.-	
RemoteServerPort	unsignedInt [0:65535]	W	The port number of the remote syslog server used for logging. RemoteServerPort is only applicable when RemoteServerEnable is true	514
LocalFilterLevel	string	W	Controls the maximum local logging level of messages locally logged. Log messages of the level specified and below are logged, all others are dropped. Logging levels are defined per RFC5424 Table 2. Enumerated list of <ul style="list-style-type: none"><li>• Emergency</li><li>• Alerts</li><li>• Critical</li><li>• Errors</li><li>• Warnings</li><li>• Notifications</li><li>• Informational</li><li>• Debugging</li></ul> Note that this affects local logging only. Remote logging always sends unfiltered log messages to the remote logging server which can filter per its requirements.	-
LocalFilterLevelEnabled	boolean	W	Logging filter enable. When false logging is not filtered, when true, local logging messages are pre-filtered.	false

Table 13. System Logging TR-069 Vendor Extensions

The “Configure System Logging” on page 14 of the CLI chapter also provides an explanation for the various logging levels.

## Time

The LocalTimeZone parameter of Device.Time requires the timezone be specified in IEEE 1003.1 (POSIX) format. This has the form EST+5 EDT,M4.1.0/2,M10.5.0/2.

This Genexis vendor extension allows operators to instead specify the time in Olson format, a much easier format to write and read. For example Europe/Berlin.

Name	Type	Write	Description	Default
Device.Time	object	-		-
X_GENEXIS_EU_LocalTimeZoneOlson	string(256)	W	<p>The local time zone definition in Olson format, e.g. Area/Location.</p> <p>The following area values are supported:</p> <ul style="list-style-type: none"> <li>• Africa</li> <li>• America</li> <li>• Antarctica</li> <li>• Asia</li> <li>• Atlantic</li> <li>• Australia</li> <li>• Etc</li> <li>• Europe</li> <li>• Indian</li> <li>• Pacific</li> </ul> <p>Location names are defined in the IANA timezone database, and are subject to occasional change. Location is the name of a specific location within the area – usually a city or small island. Country names are not used in this scheme, primarily because they would not be robust due to frequent political and boundary changes.</p> <p>The following are example values:</p> <p>Europe/Amsterdam America/New_York Africa/Cairo</p> <p>Note:</p> <ul style="list-style-type: none"> <li>• Three level names, e.g. America/Argentina/ are not supported</li> <li>• As specified by IANA, the maximum location length is 14 characters</li> </ul>	-

Table 14. Device.Time TR-069 Vendor Extensions



## CATV

Adds the ability to enable and disable CATV functionality and the ability read signal information.

Name	Type	Write	Description	Default
Device.X_GENEXIS_EU_Ext.CATV.	object	-	This object contains the Genexis vendor specific CATV information.	-
CATVInterfaceNumberOfEntries	unsignedInt	-	The number of entries in the interface table	-
Device.X_GENEXIS_EU_Ext.CATV.Interface.{i}	object	-	This object describes the characteristics of a CATV interface	-
Type	string(32)	-	Indicates the CATV module type if known. If module type is not known then "Unknown" is used	-
Enable	boolean	W	Enables or disables this CATV interface.	false
Status	string	-	Indicates the operational status of this module. An enumeration of: Disabled Enabled NotPresent Error	-
GoodOpticalSignal	boolean	-	Indicates whether good optical signal detected	-
AutomaticGainControlEnable	boolean	W	Enables or disables the AGC of this interface.	true
AutomaticGainControlStatus	string	-	Indicates the operational status of the AGC. An enumeration of: Disabled Enabled Error	-
FilterNumberOfEntries	unsignedInt	-	The number of entries in the Filter table	-
Device.X_Genexis_EU_Ext.CATV.Interface.{i}.Filter.{i}	object	-	This object describes the characteristics of a CATV interface filter	-
Enable	boolean	W	Enables or disables this filter.  Note: It is expected that only one filter is enabled at a time, else the behaviour of the CATV output is undefined.	false
Status	string	-	Indicates the operational status of this filter. Enumeration of: Disabled Enabled Error	-
Device.X_Genexis_EU_Ext.CATV.Interface.{i}.Power	object	-		-
RFOutputPower	int	-	Estimated RF output power level expressed in 0.01dBuV units Example: 8276 = 82.76 dBuV	-
OpticalInputPower	int	-	Measured Optical input power level expressed in 0.01dBm units Example: -874 = -8.74 dBm	-

Table 15. CATV TR-069 Vendor Extensions

## Bridge - IGMP

The Genexis vendor extensions to the Bridge:1 profile provide IGMP Snooping and Proxy features.

Name	Type	Write	Description	Default
Device.Bridging.Bridge.{i}.X_GENEXIS_EU_IGMP.	object	W	X_GENEXIS_EU_IGMP is the vendor extension object to manage IGMP.	-
Enabled	boolean	W	Enables or disables IGMP support.	false
ImmediateLeave	boolean	W	If enabled IGMP leave messages are suppressed from being sent upstream to the querier until the last reporter has left the group.	false
Robustness	unsignedInt[1:]	W	Robustness is a way of indicating how vulnerable the network is to lost packets. IGMP can recover from (robustness minus 1) lost IGMP packets.  RFC 3376 specifies a default of 2.	2
Aggregation	boolean	W	If enabled aggregates join and leave messages to upstream router through defined upstream service interface.	false
ClientGroupNumberOfEntries	unsignedInt	-	The number of entries in the ClientGroup table.	-
Device.Bridging.Bridge.{i}.X_GENEXIS_EU_IGMP.ClientGroup.{i}.	object	-	IGMP Client Group table reflecting the current group membership.	-
GroupAddress	string(15)	-	The IP multicast group address for which this entry contains information.	-
Version	string	-	IGMP version. Enumeration of: <ul style="list-style-type: none"> <li>v2</li> <li>v3</li> </ul>	-
Mode	string	-	IGMP mode. Enumeration of: <ul style="list-style-type: none"> <li>L2</li> <li>L3.</li> </ul>	-
Port	string(1024)	-	Path name of the interface object that this associated device is connected to e.g. Device.Ethernet.interface.2.	-
AssociatedDeviceNumberOfEntries	unsignedInt	-	The number of entries in the AssociatedDevice table.	-
Device.Bridging.Bridge.{i}.X_GENEXIS_EU_IGMP.ClientGroup.{i}.AssociatedDevice.{i}.	object	-	This table contains information about IGMP devices, typically STBs, connected to this interface.  At most one entry in this table can exist with a given value for SourceAddress.	-
SourceAddress	string(15)	-	Source address of the associated device.	-

Table 16. IGMP TR-069 Vendor Extensions

## Connecting

Controlling a CPE via TR-069 requires a working ACS (Auto-Configuration Server). The CPE subsequently needs to be configured to use this ACS.

There are two ways of configuring a CPE to use a particular ACS. The preferred way is via automatic discovery as described below. If this is not possible, the CPE can also be manually configured with the ACS's location. This process is described on page 31.



**Note:** The rest of this chapter assumes the CPE's management interface is already configured with settings permitting it to communicate with the management network. See "Configuring the Management Interface" on page 17 for an example of doing this.

---

### ACS Discovery

As defined by TR-069, the CPE indicates its support for automatic ACS discovery by sending the string "dslforum.org" in the Vendor Class Identifier (option 60) part of the DHCP client request.

The DHCP server should be configured to send the URL of the ACS server in either option 43 or option 125 of the response. This process is described in detail in "Option 43 (Vendor Specific Information)" on page 39 and "Option 125 (Vendor Identifying Vendor Specific Information)" on page 41.



**Warning:** Configure the ACS server in either option 43 or option 125, but not both. Should both options contain ACS server information, the value in option 43 will be the one used.

---

### CPE Behaviour

It is important to understand how the CPE uses ACS information supplied by either DHCP option 43 or option 125. In essence, the CPE only uses the provided information the first time it boots or after a factory reset. The implication therefore being that once a CPE has acquired the URL of an ACS, changes to that URL in subsequent DHCP offers, either on reboot or lease renewal, will not be adopted by the CPE.

This behaviour is defined by TR-069 section 3.1 (<https://www.broadband-forum.org/technical/download/TR-069.pdf>).

## Manual Configuration

When automatic discovery is not available it is necessary to manually configure the CPE with the location and connection settings of the ACS. This is done through a separate management method such as the CLI. Instructions for using the CLI are available in the chapter starting on page 7.

The example below shows how a CPE can be configured to use an ACS.

```
geneos# configure terminal
geneos(config)# cwmp acs server <http://acs.example.com>
geneos(config)# cwmp acs username <acsusername> password <acspassword>
geneos(config)#
```

At a minimum, the CPE needs to know the IP address or hostname of the ACS and the username and password with which to connect.

For a full list of configurable ACS settings, use the CLI's help features as explained in "Getting help" on page 10.

## Tasks

### Checking product information

Use an ACS to access the object `Device.DeviceInfo.SoftwareVersion`.

### Changing the default password

A list of users is available by accessing the user table in `Device.Users` from an ACS. Determine the appropriate row and write to the `Password` field.

For example, if "operator" is the first entry in the user table, change the password for that account by writing the new password to `Device.Users.User.0.Password`.

### Changing the hostname

The `Device.DeviceInfo.X_GENEXIS_EU_Hostname` object can be used to change the hostname.

### Setting the date and time

Use the `Device.Time.NTPServerX` object (where *X* is a number from 1 to 5 inclusive) to provide a list of NTP servers.

Use the `Device.Time.X_GENEXIS_EU_LocalTimeZoneOlson` object to specify the correct timezone in Olson (Area/Location) format.

### Configure System Logging

Use the `Device.X_GENEXIS_EU_Ext.Logging` object to specify an external syslog server and configure local logging options.

### Viewing current (active) configuration

CWMP contains no single-step way to do this. The ACS should be used to query the relevant settings.

### Saving the current configuration

The configuration is typically saved automatically by the ACS when the session is terminated.

## Upgrading firmware or bootloader

Both the firmware and bootloader can be upgraded using the Download RPC method. The TargetFileName parameter is used to differentiate between a firmware upgrade and a bootloader upgrade. For the changes to take effect the CPE needs to be rebooted. Under normal circumstances the CPE will initiate the reboot.

The following table shows the values that need to be provided to certain command parameters.

Upgrade Type	Parameter	
	FileType	TargetFileName
Firmware	"1 Firmware Upgrade Image"	"bootflash" <b>or</b> "" (empty string)
Bootloader	"1 Firmware Upgrade Image"	"bootloader"

Table 17. Parameters for upgrading via CWMP

The full syntax of the command is described in "TR-069 Amendment 5"  
([https://www.broadband-forum.org/technical/download/TR-069\\_Amendment-5.pdf](https://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf)).

## Rebooting

Use the Reboot RPC method as described in "TR-069 Amendment 5"  
([https://www.broadband-forum.org/technical/download/TR-069\\_Amendment-5.pdf](https://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf)).

## Configuring the Management Interface

While technically possible to configure the management interface via CWMP , doing so is beyond the scope of this document.

The IP address of the CPE's management interface can be assigned manually or by DHCP server.

In addition to providing an IP address, the server can be configured to send additional settings to the CPE using various DHCP options. The purpose of this chapter is to describe the DHCP request process and the options that the CPE can receive from the DHCP server.

The DHCP process is initiated under the following conditions:

- When the CPE powers up or reboots.
- When the CPE renews its IP address.



**Note:** The DHCP server configuration examples in this chapter are taken from the ISC DHCP server.  
(<https://www.isc.org/downloads/dhcp/>)

## Connecting

For the CPE to make use of information supplied via DHCP, it has to be configured to acquire its IP address from a DHCP server. If the IP address has been configured manually, no DHCP process takes place. To check the active configuration of the WAN interface, see "Viewing current (active) configuration" on page 16. To change the WAN interface configuration, see "Configuring the Management Interface" on page 17.



**Note:** The default (factory) setting is for the CPE to acquire its IP address via DHCP.

## DHCP Request Process

When the CPE initiates the DHCP process with either a DHCP DISCOVER (on power up or reboot) or DHCP REQUEST (on renewal) it includes several options that can be used to affect the DHCP server's response.

The following table lists the options included in the DHCP client request that will be discussed in this document:

Option	Description
55	Parameter List
60	Vendor Class Identifier
61	Client Identifier

Table 18. Options included in DHCP client request

## Option 55 (Parameter List)

This is used by the CPE to list all the options that it will accept from the DHCP server.

The options listed here fall into two categories:

1. Compulsory options that the server must provide
2. Supplemental options. It is not necessary to provide them, but when used, can provide the CPE with additional configuration information.

The first table below lists the required options. Failure to supply all of these options will result in a non-functioning device.

The second table lists those options that can be used to provide supplemental information to the CPE (such as a hostname), or information required to enable specific features such as automatic ACS discovery.

Name	Example
1 (netmask)	option subnet-mask 255.255.255.0;
3 (routers)	option routers 192.168.42.254;
6 (dns-server)	option domain-name-servers 192.168.42.249, 192.168.42.248;
15 (domain-name)	option domain-name "example.com";

Table 19. Required DHCP Options

Name	Example
43 (vendor-info)	(see page 39)
125 (V-I Vendor-specific Information)	(see page 41)

Table 20. Optional DHCP Options



## Option 60 (Vendor Class Identifier)

This is a free form text field that can be used to send information from the CPE to a DHCP server. The DHCP server parses this string and then based on the contents, can selectively send particular configuration options to specific CPEs. It is up to individual operators to determine the format of this string and the effect of each component.

As each VLAN is capable of obtaining its own IP address, option 60 is set on a per VLAN basis.

Using the CLI, the contents of this string can be fully customised.

```
geneos# configure terminal
geneos(config)# interface vlan1
geneos(config-if-vlan)# dhcp client send-option 60 dslforum.org,mgmt,plat-7840
```

A syntactic alternative for this command exists. Instead of specifying the option number, the option name can be provided:

```
geneos# configure terminal
geneos(config)# interface vlan1
geneos(config-if-vlan)# dhcp client send-option vendor-class-identifier dslforum.org,mgmt,plat-7840
```



**Warning:** For ACS discovery to work, the vendor class identifier must include the string "dslforum.org".

---

## Option 61 (Client Identifier)

All devices requesting an IP address from a DHCP server provide their unique identifier in option 61. The purpose of this identifier is to allow the DHCP server to uniquely identify individual devices and to provide them with settings customised for that device.

GenesOS formats the client identifier according to RFC 3315. A typical identifier looks as follows:

```
ff0001000100030001000f94ba2a42
```

To discover the client ID used by a particular interface, use the CLI to run the **show dhcp client lease** command.

```
geneos# show dhcp client lease
      Interface : vlan1
      MAC Address :
      IP Address : 192.168.42.1
      Vendor Class Id : genes-lunar-3.0.0-R,lunar,platinum-7840,dslforum.org
      Client-ID : ff0001000100030001000f94ba2a42
      Server-ID : 192.168.42.254
      Next Server : 192.168.42.254
```

## Assigning a Static IP to a CPE

Some operators find it desirable to use DHCP to consistently assign the same IP address to a particular CPE. This can be done by configuring the DHCP server with a static mapping (also known as a reservation).

The following example shows how this identifier can be used in the ISC DHCP server to send a static IP (192.168.42.6) to a specific CPE.

```
host CPE42 {
    option dhcp-client-identifier ff:00:01:00:01:00:03:00:01:00:0f:94:ba:2a:42;
    fixed-address 192.168.42.6;
}
```

The typical method of using the hardware ethernet parameter in the host{ } section will still work, but you lose the flexibility and fine grained control afforded by using the client ID.

Instructions for configuring a static mapping on a Microsoft DHCP server can be found in the section "Creating a Reservation (static mapping)" on page 48 of "Appendix B. DHCP for Windows".

## DHCP Server Response

Alongside an IP address, DHCP server responses contain a multitude of extra information such as DNS servers, lease times and domain names. Configuring these options is part of regular DHCP server administration and is not covered in this document.

Of particular interest to operators is the ability to use DHCP to provide CPEs with ACS information.

This information is provided via options 43 or 125. The rest of this chapter shows how to configure these two options.



**Warning:** Configure ACS server information in either option 43 or option 125, but not both. Should both options contain ACS server information, the value in option 43 will be the one used.

## Using DHCP for ACS Discovery

When using DHCP for ACS discovery, it is important to understand how the CPE processes the information supplied by the DHCP server. The CWMP chapter contains a section “CPE Behaviour” on page 30 that explains this in detail.

This chapter only concerned with configuring DHCP.

## Option 43 (Vendor Specific Information)

This option is used to provide the CPE with information about the location of the ACS used for managing the CPE via CWMP.

This information has four components. The follow table lists these components, their data type and whether or not their inclusion is required.

Code	Name	Description	Required
1	ACS	The URL of the ACS	YES
2	Provisioning Code	An operator defined string used by the ACS server to group CPEs.	no
3	Minimum Wait Interval	CWMP session retry minimum wait interval	no
4	Retry Interval Multiplier	The initial value of the CWMP session retry interval multiplier	no

Table 21. Broadband Forum Option 43 codes  
([https://www.broadband-forum.org/technical/download/TR-069\\_Amendment-5.pdf](https://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf))

## Configuring the ISC DHCP server

Configuring the ISC DHCP server to provide data in option 43 is done in two steps:

1. Declare an option space and define the name, code and data type of each component.
2. Provide values for each of the components.

### 1. Declare option space.

These lines must be placed in the global scope.

```
option space bbf;  
option bbf.acs code 1 = text;  
option bbf.provisioningcode code 2 = text;  
option bbf.minwaitinterval code 3 = unsigned integer 32;  
option bbf.retryintervalmultiplier code 4 = unsigned integer 32;
```

In the above example, an option space called "bbf" has been declared. The four components of the ACS data (as described in "Table 21. Broadband Forum Option 43 codes" on page 39) are then listed and their data types defined.

### 2. Provide values for each component.

While it is possible to add these lines as global parameters, it is strongly advised they be put in subnet, pool or group scope.

```
vendor-option-space bbf;  
option bbf.acs "http://192.168.42.239:8080/acs";  
option bbf.provisioningcode "provisioning code value";  
option bbf.minwaitinterval 500;  
option bbf.retryintervalmultiplier 4000;
```

The first line above tells the DHCP server to send the information in the "bbf" option space as option 43. The next four lines set the values for each of the ACS data component parts.

The value for the optional "provisioning code" field is determined by the operator. How or if this value is used is also determined by the operator.

## Option 125 (Vendor Identifying Vendor Specific Information)

Option 125 is an alternative method for providing the CPE with ACS location information.

Configuring option 125 is very similar to option 43. The primary difference is that all the options defined by each specific vendor are grouped together in a subgroup. This prevents potential collisions if multiple vendors all use the same particular code.

There are two sets of information required by option 125:

1. The ACS settings needed by the CPE in order for it to function as required.
2. The vendor ID used to group all the settings provided in step 1.

The following table lists the ACS settings that can be provided and specifies the vendor ID needed to group them.

Code	Name	Description	Required
11	ACS	The URL of the ACS	YES
12	Provisioning Code	An operator defined string used by the ACS server to group CPEs.	no
13	Minimum Wait Interval	CWMP session retry minimum wait interval	no
14	Retry Interval Multiplier	The initial value of the CWMP session retry interval multiplier	no

Table 22. Broadband Forum Option 125 codes  
([https://www.broadband-forum.org/technical/download/TR-069\\_Amendment-5.pdf](https://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf))



**Warning:** The ACS codes used for option 43 are not the same as the codes used for option 125!

The following table shows the Vendor ID used to encapsulate the ACS parameters in Table 22.

Vendor ID	Vendor Name
3561	Broadband Forum

Table 23. Vendor ID for encapsulating ACS parameters

### Configuring the ISC DHCP server

Configuring option 125 in the ISC DHCP server is done in four steps:

1. Declare an option space that declares the name, code and type of each ACS parameter.
2. Declare a vendor option space that will be used to group the options in step 1.
3. Encapsulate the ACS parameters option space in the vendor option space and the vendor option space in option 125.
4. Assign each of the ACS parameters a value.

## 1. Declare option space for the ACS parameters

These lines need to be placed in global scope.

```
option space bbf;  
option bbf.acs code 11 = text;  
option bbf.provisioningcode code 12 = text;  
option bbf.minwaitinterval code 13 = unsigned integer 32;  
option bbf.retryintervalmultiplier code 14 = unsigned integer 32;
```

The first line above declares the option space. The following lines specify each parameter, its code and data type.

## 2. Declare the vendor option space

This line must also go in global scope.

```
option space vivso code width 4;
```

Specifying code width 4 is mandatory otherwise the DHCP server will send out malformed packets.

## 3. Encapsulate the option space

This is also to be placed in global space.

```
option vivso.bbf code 3561 = encapsulate bbf;  
option option125 code 125 = encapsulate vivso;
```

The first line groups all the ACS parameters together under the vendor ID 3561. This ID belongs to the Boadband Forum who define the layout and codes used for ACS discovery.

The second line then encapsulates all the information in the vendor ID into option 125.

## 4. Assign a value to the ACS parameters

The configuration lines below should be placed in subnet, group or pool scope.

```
option bbf.acs "http://192.168.42.239:8080/acs";  
option bbf.provisioningcode "provisioning code value";  
option bbf.minwaitinterval 500;  
option bbf.retryintervalmultiplier 4000;
```

At the time of writing, there is a bug in ISC DHCP that requires the following two lines be added in global scope in order for the DHCP server to actually include option 125 in its offer.

```
option vivso.iana code 0 = string;  
option vivso.iana 01:01:01;
```

## Complete Listing

Below is the complete listing of the configuration required for option 125 (including work around).

```
# GLOBAL SCOPE
option space bbf;
option bbf.acs code 11 = text;
option bbf.provisioningcode code 12 = text;
option bbf.minwaitinterval code 13 = unsigned integer 32;
option bbf.retryintervalmultiplier code 14 = unsigned integer 32;

option space vivso code width 4;
option vivso.iana code 0 = string;
option vivso.iana 01:01:01;

option vivso.bbf code 3561 = encapsulate bbf;
option option125 code 125 = encapsulate vivso;

# SUBNET, POOL OR GROUP SCOPE
option bbf.acs "http://192.168.42.239:8080/acs";
option bbf.provisioningcode "provisioning code value";
option bbf.minwaitinterval 500;
option bbf.retryintervalmultiplier 4000;
```

## Verifying DHCP options passed to the CPE

To verify exactly what the CPE is receiving from the DHCP server (via option 43 or option 125), connect to the CPE via SSH and use the command line (explained in the chapter “Option 43 (Vendor Specific Information)” on page 39).

```
geneos# show dhcp client lease
      Interface : vlan1
      MAC Address :
      IP Address : 192.168.42.1
      Vendor Class Id : geneos-lunar-3.0.0-R,lunar,platinum-7840,dslforum.org
      Client-ID : ff0001000100030001000f94ba2a42
      Server-ID : 192.168.42.254
      Next Server : 192.168.42.254
      File :
      Renew in : 0h0m0s
      Rebind in : 0h0m0s
      Expire in : 0h6m46s
      DHCP Options :
      Option 1 : netmask 255.255.255.0
      Option 3 : routers 192.168.42.254
      Option 6 : dns-server 192.168.42.254
      Option 12 : hostname CPE-42
      Option 15 : domain-name example.com
      Option 28 : broadcast
      Option 43 : vendor-info
      Option 125 : V-I Vendor-specific Information 0003014F4F4040400000004
```

## Tasks

### Checking product information

A limited amount of information such as platform, firmware version and MAC address can be gleaned from the contents of the DHCP DISCOVER packet (particularly option 60).

A far more comprehensive list of details can be viewed via the command line. See “Checking product information” on page 12.

### Changing the hostname

A CPE’s hostname cannot be set over DHCP.

### Other tasks

DHCP is not capable of querying the CPE, so to view the running configuration, an alternative method such as the CLI will need to be used. See “Viewing current (active) configuration” on page 16.

Settings acquired via DHCP are used only as long as the DHCP lease is valid. It is not possible to save these settings.

DHCP cannot be used to change passwords, upgrade the firmware or bootloader or reboot the device. Another method (such as the CLI) must be used.



# Appendix A. DHCP Client ID

A typical Genexis DHCP Client Identifier looks as follows:

```
FF0001000100030001000F94BA2A42
```

The rest of this chapter breaks down the Client ID into its component parts and describes what they are.

The format for the CID as a whole is specified in section 6.1 of RFC 4361.

This RFC breaks down the CID into the following three components. These components are further analysed in the rest of this chapter.

Type	IAID				DUID									
0	1	3	4	5	6	7	8	9	10	11	12	13	14	15
FF	00	01	00	01	00	03	00	01	00	0F	94	BA	2A	42

## Type

Byte 0.

RFC 4361 defines a value of 0xFF in this field as indicating that the CID is an RFC 3315-style binding identifier.

This further determines the rest of the identifier format. The type field must be followed by a four byte IAID field (see below) and then by a DUID field (also see below) of optional length.

## IAID (Interface Association Identifier)

Bytes 1 - 5.

RFC 4361 defines the 32 bit IAID field as being of "opaque type". This means the purpose of each bit is determined by the vendor, in this case, Genexis.

This field is composed in "network byte order" or Big Endian format.

Reserved								Interface Index				Interface Type				Reserved				VLAN ID											
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Bit	Name	Description
31-24	Reserved	
23-20	Interface Index	0: a native interface such as vlan1 1: a /1 virtual (sub) interface such as vlan1/1 2: a /2 virtual (sub) interface such as vlan1/2 3: a /3 virtual (sub) interface such as vlan1/3 4: a /4 virtual (sub) interface such as vlan1/4
19-16	Interface Type	0: reserved 1: upstream 2: downstream 3: wireless 4-7: reserved
15-12	Reserved	
11-0	VLAN ID	The VLAN through which the DHCP request passes.

Table 24. IAID bit fields

## DUID (DHCP Unique Identifier)

Bytes 6 - 15.

The format of this section is specified by RFC 3315 section 9.

Genexis has chosen to use the DUID-LL format. This means the DUID is based on link-layer address.

DUID Type		Hardware Type Code		Link Layer Address					
0	1	2	3	4	5	6	7	8	9
00	03	00	01	00	0F	94	BA	2A	42

Byte	Name	Description
0-1	DUID Type	RFC 3315 specifies three different DUID formats. We use the third type (DUID-LL) and this is indicated here by specifying a DUID Type of 3. It is a two byte field.
2-3	Hardware Type Code	The hardware type code is defined by RFC 826 and is written in network (big-endian) order.
4-9	Link Layer Address	This is the MAC address of the interface from which the DHCP request originates.

Table 25. DUID byte fields

## Appendix B. DHCP for Windows

---

A Windows DHCP Server can be used to dynamically assign IP addresses and other configuration information to CPEs.

The more common options (such as subnet mask, gateway, DNS etc) can be easily configured through the usual widget.

The other options of relevance to operators include option 43 and 125. These options are used for automatic ACS discovery.

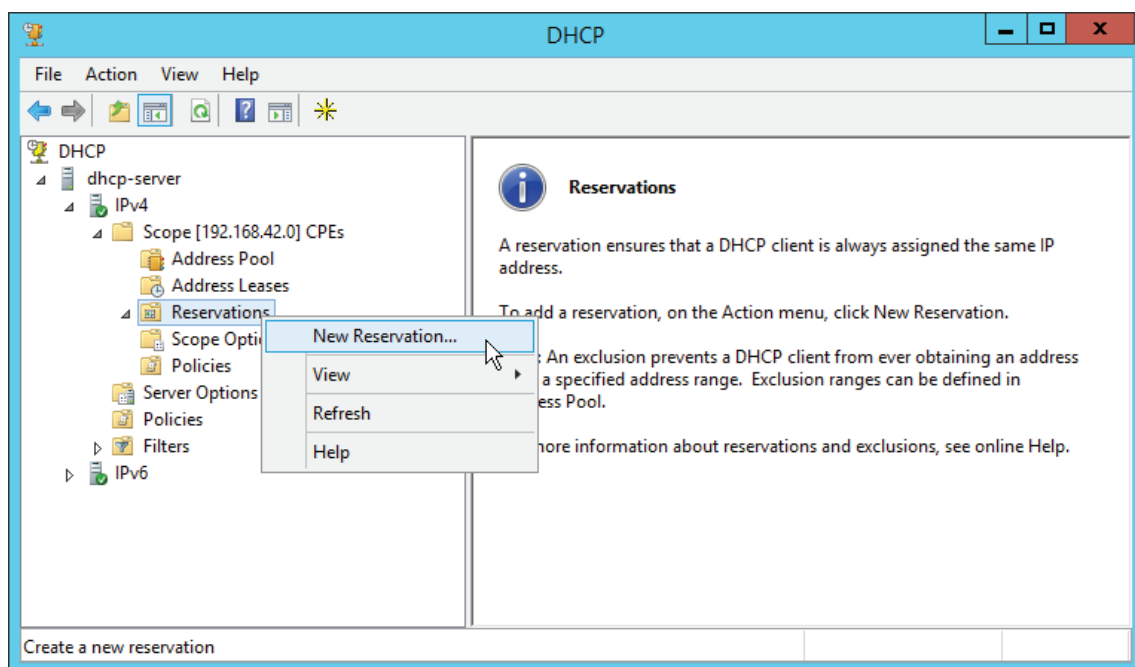
The purpose of this chapter is to demonstrate how to perform the following two tasks on a Microsoft Windows DHCP server:

1. Create a reservation (static IP mapping)
2. Configure option 43 and 125.

In all of the following examples it is assumed that the Windows DHCP service has already been installed and in a working state. These instructions deal only with the specific topics mentioned above.

### Creating a Reservation (static mapping)

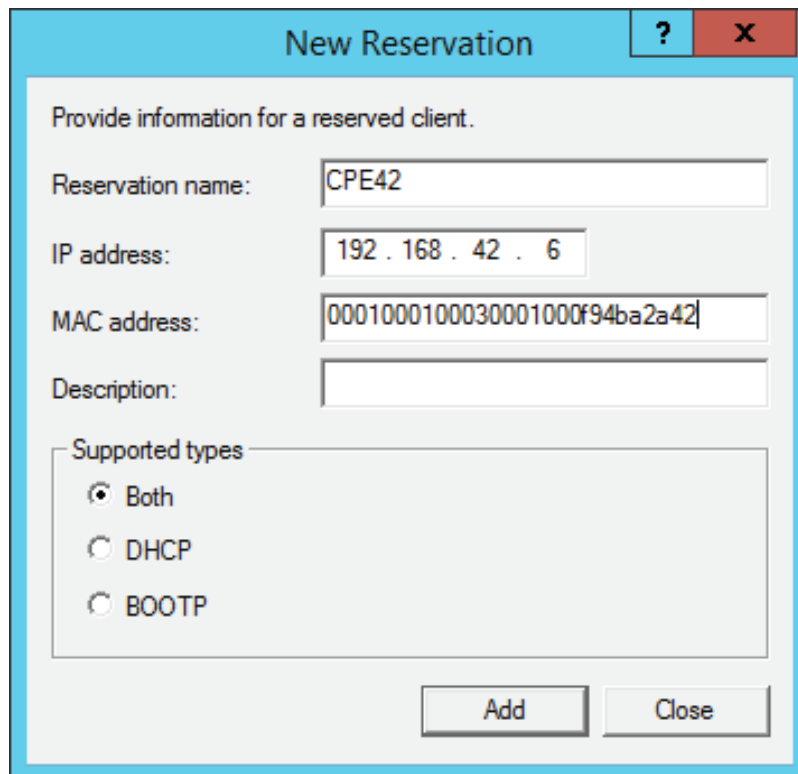
Expand the scope in which you wish to add the static mapping.  
Find the "Reservation" entry and right click it.



Choose "New Reservation".

Fill in a reservation name and the static IP address you want applied to the specific device. In the MAC address line, fill in the client ID **without the leading FF**.

Click on "Add".

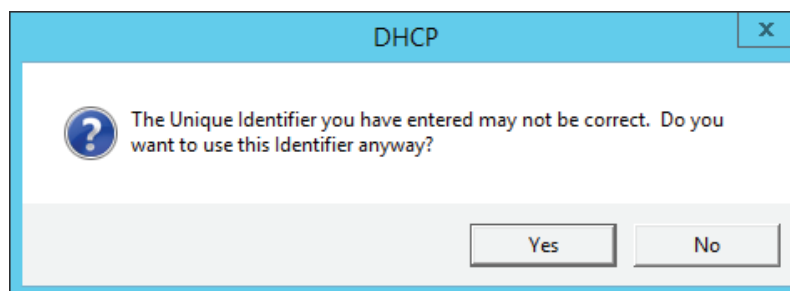


The "New Reservation" dialog box is shown with a light blue title bar and a red close button. It contains the following fields and options:

- Reservation name: CPE42
- IP address: 192 . 168 . 42 . 6
- MAC address: 0001000100030001000f94ba2a42
- Description: (empty)
- Supported types:
  - ☒ Both
  - ☐ DHCP
  - ☐ BOOTP

Buttons at the bottom: Add, Close.

You will then be presented with a warning message as show below.



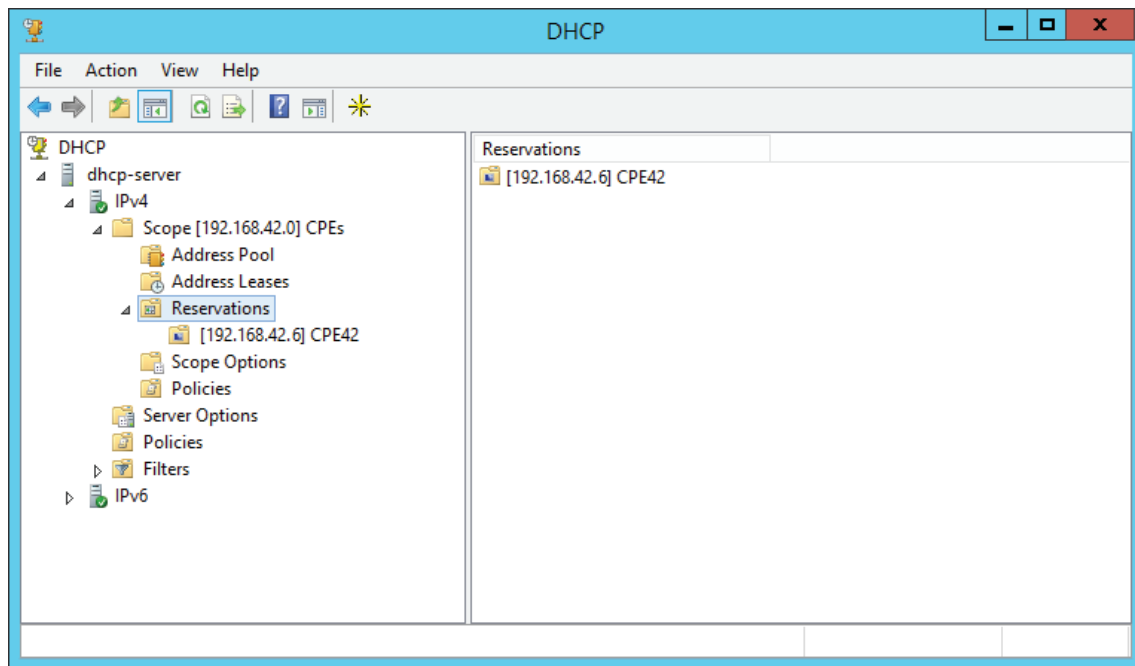
The "DHCP" warning dialog box is shown with a light blue title bar and a red close button. It contains the following text and buttons:

**?** The Unique Identifier you have entered may not be correct. Do you want to use this Identifier anyway?

Buttons at the bottom: Yes, No.

Click on "Yes". Contrary to the message, the identifier is indeed correct.

You will then be returned to the DHCP server overview. You will see the new static mapping in the list of reservations.



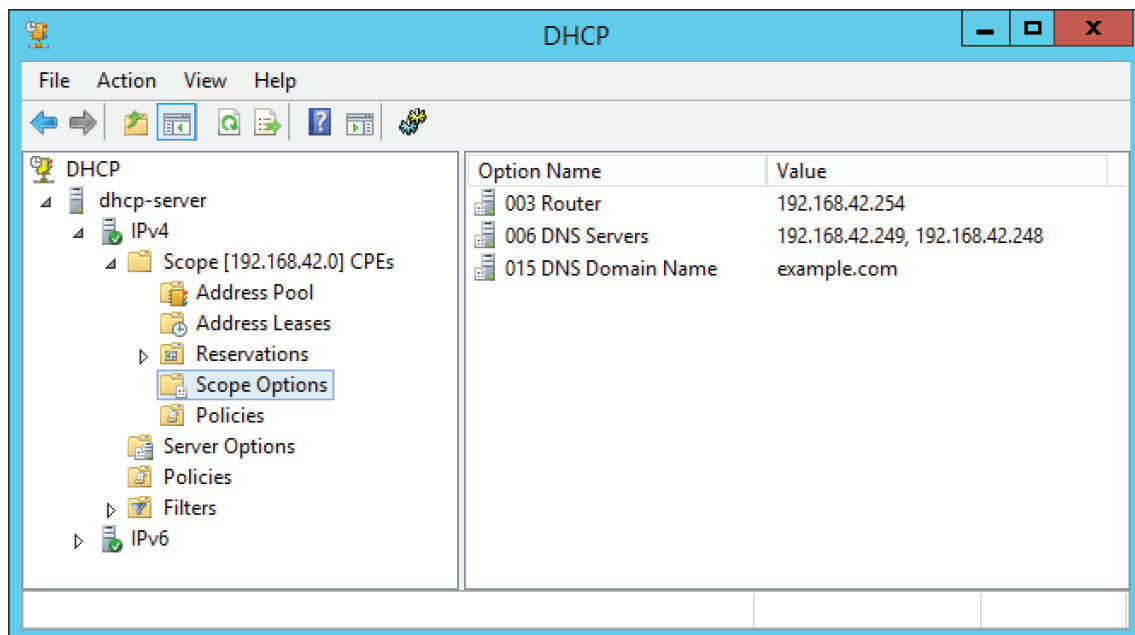
**Tip:** If you find your reservation isn't working, make sure the MAC address field does not contain the leading FF!

## Sending Vendor Specific Options

Configuring option 43 and 125 is considerably more complicated on a Windows system than other systems. The operator must manually convert all field values to hexadecimal, calculate field lengths (in hexadecimal) and then construct the payload. The whole process is very error prone and difficult to debug. For this reason it is strongly recommended that operators choose a Unix based system.

Stage 1 involves converting all field values into hexadecimal and constructing the option payload from the results.

Stage 2 entails configuring the DHCP service with the payload constructed in stage 1.



## Option 43

For an introduction as to how option 43 is structured, please refer to the section “Option 43 (Vendor Specific Information)” on page 39.

### Stage 1: Constructing the Payload

The goal is to create a single hexadecimal string containing all the encoded vendor options.

The format of the string is as follows:

```
<option><length of data><data>  
<option><length of data><data>  
.  
.  
.
```

That line is repeated as many times as necessary to encode all required options.

The procedure for calculating the string takes a “bottom up” approach and is as follows:

1. For each individual option:
  - 1.1. Convert the option value into a hexadecimal string.
  - 1.2. Count the number of bytes in the string and convert that value to hexadecimal.
  - 1.3. Convert the option number to hexadecimal.
  - 1.4. Concatenate each of the values derived in the previous 3 steps into a single string. The order is important! The value found in step 3 must be prepended to the value found in step 2 which in turn is prepended to value derived in step 1.
2. Join all the individual option strings together (order is not important).

The following table shows each value that needs to be encoded and the vendor ID that they’re all going to be grouped under. This information will be used in this working example.

Description	Code	Value
ACS location	1	http://192.168.42.239:8080/acs
Provisioning Code	2	provisioning code value
Min Wait Interval	3	500
Retry Interval Multiplier	4	4000

Table 26. Data for option 43



Step 1. Calculate option strings.

**For the ACS field:**

1. Convert the value into hexadecimal.

```
h t t p   / / 1 9 2 . 1 6 8 . 4 2 . 2 3 9 : 8 0 8 0 / a c s
68 74 74 70 3A 2F 2F 31 39 32 2E 31 36 38 2E 34 32 2E 32 33 39 3A 38 30 38 30 2F 61 63 73
```

2. Count the number of bytes (30) and convert that to hexadecimal (0x1E). Note: you must convert the actual number, not the ASCII representation of it.

```
30
1E
```

3. Convert the option code (1) to hexadecimal (0x01). Note: you must convert the actual number, not the ASCII representation of it.

```
01
01
```

4. Concatenate the results from step 3, step 2 and step 1 (in that order).

```
01 30 h t t p   / / 1 9 2 . 1 6 8 . 4 2 . 2 3 9 : 8 0 8 0 / a c s
01 1E 68 74 74 70 3A 2F 2F 31 39 32 2E 31 36 38 2E 34 32 2E 32 33 39 3A 38 30 38 30 2F 61 63 73
```

### For the provisioning code field:

1. Convert the value into hexadecimal.

```
p r o v i s i o n i n g   c o d e   v a l u e
70 72 6F 76 69 73 69 6F 6E 69 6E 67 20 63 6F 64 65 20 76 61 6C 75 65
```

2. Count the number of bytes (23) and convert that to hexadecimal (0x17). Note: you must convert the actual number, not the ASCII representation of it.

```
23
17
```

3. Convert the option code (2) to hexadecimal (0x02). Convert the number, not the ASCII representation.

```
2
02
```

4. Concatenate the results from step 3, step 2 and step 1 (in that order).

```
2 23 p r o v i s i o n i n g   c o d e   v a l u e
02 17 70 72 6F 76 69 73 69 6F 6E 69 6E 67 20 63 6F 64 65 20 76 61 6C 75 65
```

### For the Min Wait Interval field:

1. Convert the value to hexadecimal. Note: you need to convert the actual number, not the hexadecimal representation of it.

The BroadBand Forum (the body that defined the format of these options) specified that this field is always four bytes in length. So once you've converted the number, the result needs to be padded with zeroes until it's four bytes in length.

```
      500
00 00 01 F4
```

2. The number of bytes is fixed at four, so no counting is necessary

```
  4
04
```

3. Convert the option code (3) to hexadecimal (0x03). Convert the number, not the ASCII representation.

```
  3
03
```

4. Concatenate the results from step 3, step 2 and step 1 (in that order).

```
  3  4      500
03 04 00 00 01 F4
```

## For the Retry Interval Multiplier

1. Convert the value to hexadecimal. Note: you need to convert the actual number, not the hexadecimal representation of it.

This field is also specified by the BBF to always be four bytes in length. The converted value therefore needs to be padded to that length.

The BBF also specifies that this value must fall in the range 1000 - 65535 (<https://www.broadband-forum.org/cwmp/tr-181-2-9-0.html>).

```
      4000
00 00 0F A0
```

2. The length is fixed at four bytes by the specification.

```
      4
00 00 00 04
```

3. Convert the option code (4) to hexadecimal (0x04). Convert the number, not the ASCII representation.

```
      4
04
```

4. Concatenate the results from step 3, step 2 and step 1 (in that order).

```
      4  4      4000
04 04 00 00 0F A0
```

Step 2. Join all the option strings together

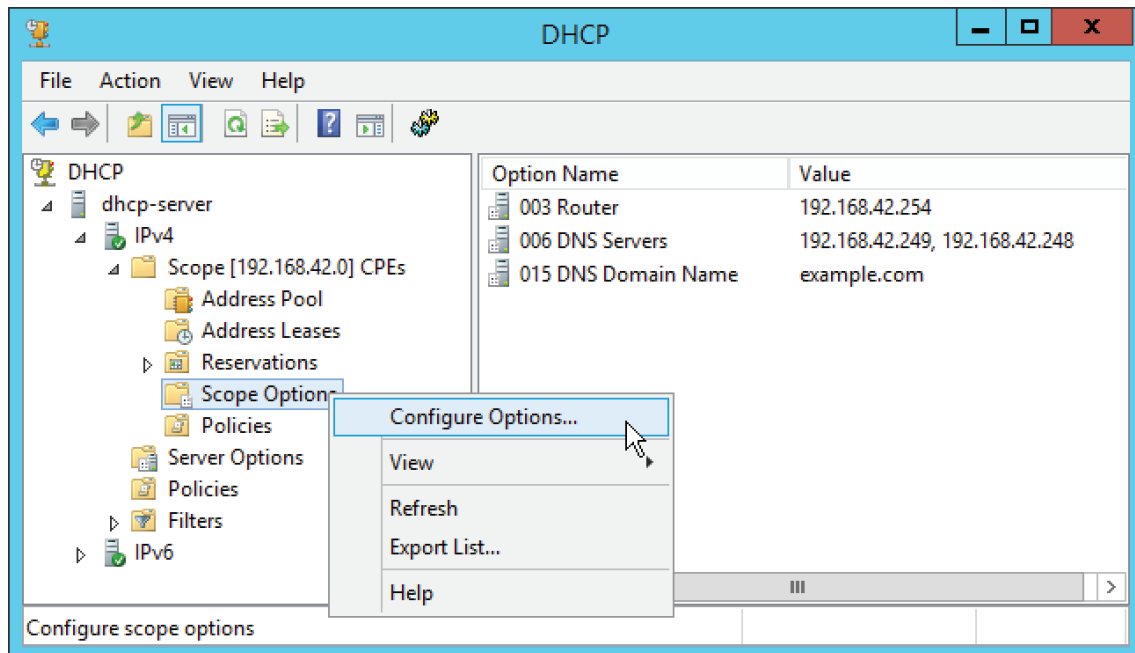
Take each of the strings calculated at step 4 for each of the options above and join them together. The order is not important.

```
1 30 h t t p / / 1 9 2 . 1 6 8 . 4 2 . 2 3 9 : 8 0 8 0 / a c s
2 23 p r o v i s i o n i n g c o d e v a l u e 3 4 500 4
4 4000
```

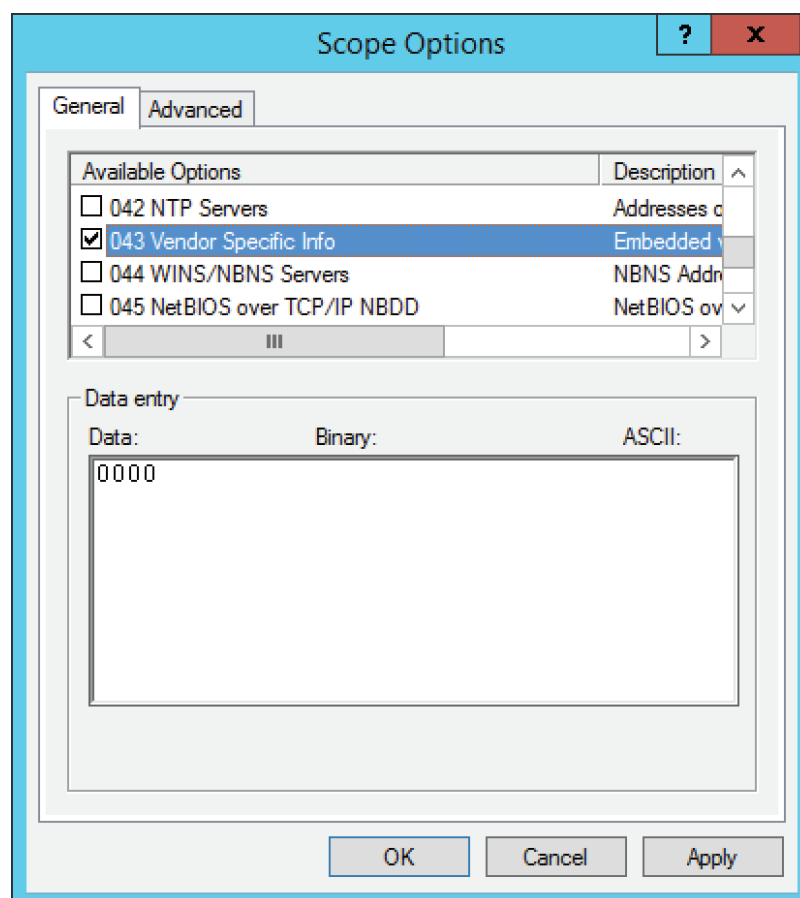
```
01 1E 68 74 74 70 3A 2F 2F 31 39 32 2E 31 36 38 2E 34 32 2E 32 33 39 3A 38 30 38 30 2F 61 63 73
02 17 70 72 6F 76 69 73 69 6F 6E 69 6E 67 20 63 6F 64 65 20 76 61 6C 75 65 03 04 00 00 01 F4 04
04 00 00 0F A0
```

## Stage 2: Configuring Windows DHCP Server

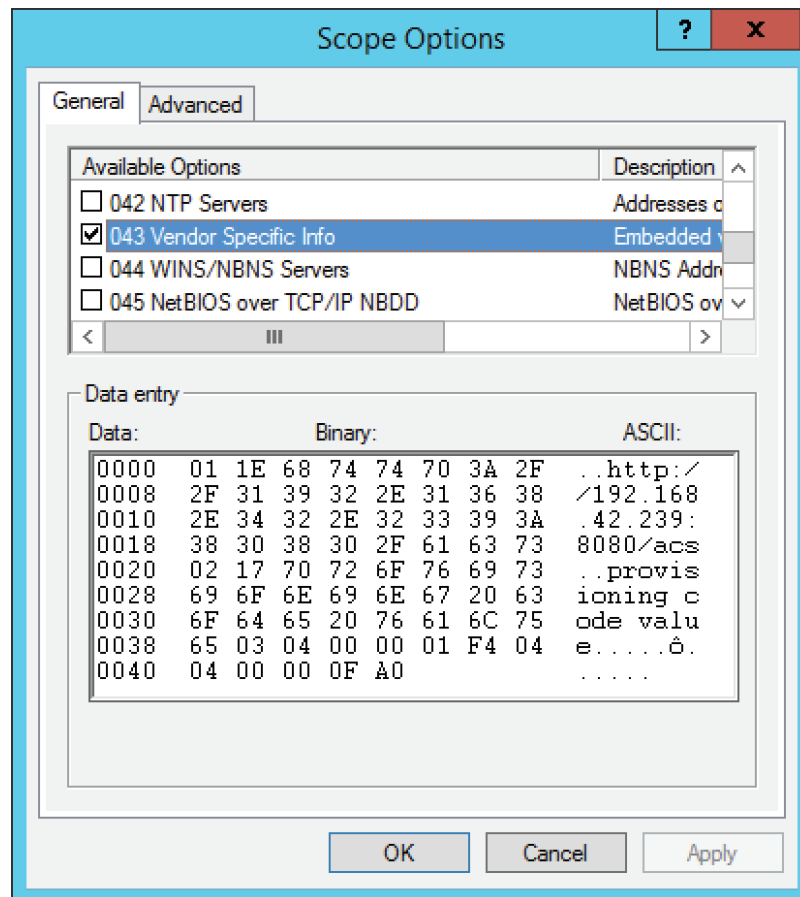
Step 1. Right click "Scope Options" and choose "Configure Options".



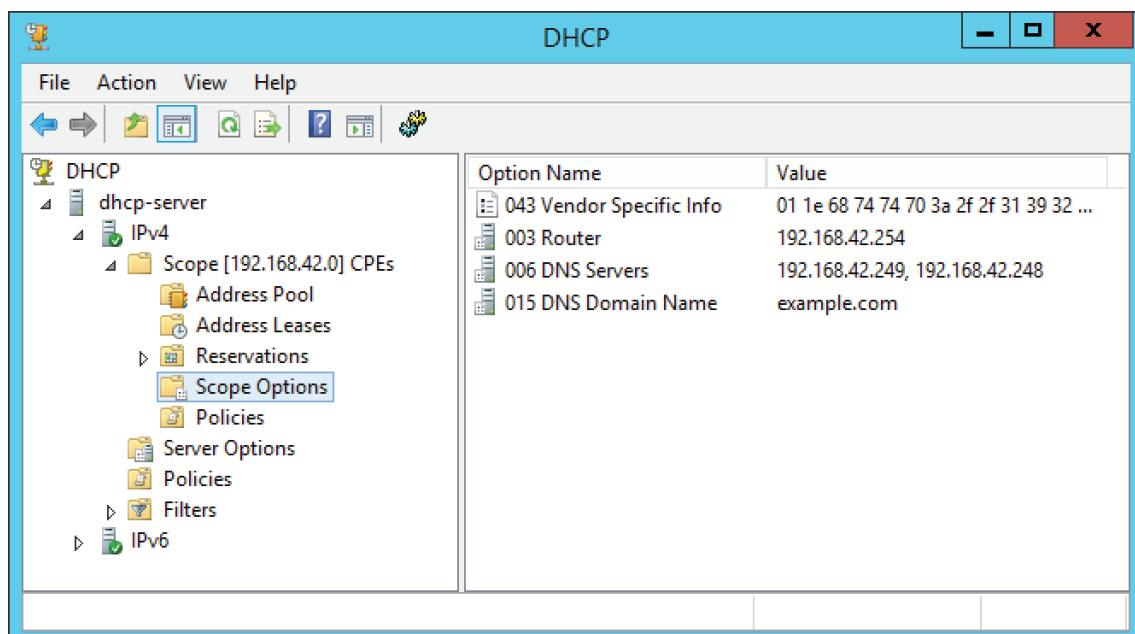
Step 2. Scroll down until you find option "043 Vendor Specific Info". Tick the box to make it active.



- Step 3. Place the cursor in the text field under the "Binary" column heading. Type in the text calculated at the final step of stage 1. Click "Apply".



You'll now see option 43 present in the server options list.





**Note:** You cannot simply copy and paste these examples and change the option values. You need to perform all steps as detailed in this document in order to calculate the length values that will be unique to your settings.

To test option 43 has been configured correctly, use the CLI interface of the CPE to run debugging commands such as:

```
show running-config
show cwp status
show dhcp client lease
```



## Option 125

For an introduction as to how option 125 is structured, please refer to the section “Option 125 (Vendor Identifying Vendor Specific Information)” on page 41.

### Stage 1: Constructing the Payload

The goal is to create a single hexadecimal string containing all the vendor encoded options.

The format of the string is as follows:

```
<vendor ID><length of vendor data>  
<option><length of data><data>  
<option><length of data><data>  
.  
.  
.
```

The last line is repeated as many times as necessary for the given vendor ID.

The whole structure is repeated as many times as necessary to include all the different vendors as required.

The procedure for calculating the string takes a “bottom up” approach and is as follows:

1. For each individual option:
  - 1.1. Convert the option value into a hexadecimal string.
  - 1.2. Count the number of bytes in the string and convert that value to hexadecimal.
  - 1.3. Convert the option number to hexadecimal.
  - 1.4. Concatenate each of the values derived in the steps into a single string. The order is important! The value found in step 3 must be prepended to the value found in step 2 which in turn is prepended to value derived in step 1.
2. Join all the individual option strings together (order is not important).
3. Count the number of bytes in the entire string and convert the value to hexadecimal. Note: it is not enough to simply sum all the values found in step 1.2. Count the number of bytes in the string and convert that value to hexadecimal. That sum does not take into account the fact that the entire string also contains the length and code value for each option.
4. Convert the vendor ID to hexadecimal.
5. Create the final string by concatenating (in this order) the vendor ID from step 4. Convert the vendor ID to hexadecimal., the byte count calculated in step 3. Count the number of bytes in the entire string and convert the value to hexadecimal. Note: it is not enough to simply sum all the values found in step 1.2. Count the number of bytes in the string and convert that value to hexadecimal. That sum does not take into account the fact that the entire string also contains the length and code value for each option.

If necessary, the whole process as listed above needs to be repeated for each vendor whose options need to be included in option 125.

The following table shows each value that needs to be encoded and the vendor ID that they're all going to be grouped under. This information will be used in this working example.

Option			
Vendor ID	Description	Code	Value
3561	ACS location	11	http://192.168.42.239:8080/acs
	Provisioning Code	12	provisioning code value
	Min Wait Interval	13	500
	Retry Interval Multiplier	14	4000

Table 27. Data for option 125

Step 1. Calculate option strings.

### For the ACS field:

1. Convert the value into hexadecimal.

```
h t t p   / / 1 9 2 . 1 6 8 . 4 2 . 2 3 9 : 8 0 8 0 / a c s
68 74 74 70 3A 2F 2F 31 39 32 2E 31 36 38 2E 34 32 2E 32 33 39 3A 38 30 38 30 2F 61 63 73
```

2. Count the number of bytes (30) and convert that to hexadecimal (0x1E). Note: you must convert the actual number, not the ASCII representation of it.

```
30
1E
```

3. Convert the option code (11) to hexadecimal (0x0B). Note: you must convert the actual number, not the ASCII representation of it.

```
11
0B
```

4. Concatenate the results from step 3, step 2 and step 1 (in that order).

```
11 30 h t t p   / / 1 9 2 . 1 6 8 . 4 2 . 2 3 9 : 8 0 8 0 / a c s
0B 1E 68 74 74 70 3A 2F 2F 31 39 32 2E 31 36 38 2E 34 32 2E 32 33 39 3A 38 30 38 30 2F 61 63 73
```

### For the provisioning code field:

1. Convert the value into hexadecimal. Each byte needs to be separated with a ":".

```
p r o v i s i o n i n g   c o d e   v a l u e
70 72 6F 76 69 73 69 6F 6E 69 6E 67 20 63 6F 64 65 20 76 61 6C 75 65
```

2. Count the number of bytes (23) and convert that to hexadecimal (0x17). Note: you must convert the actual number, not the ASCII representation of it.

```
23
17
```

3. Convert the option code (12) to hexadecimal (0x0C). Convert the number, not the ASCII representation.

```
12
0C
```

4. Concatenate the results from step 3, step 2 and step 1 (in that order).

```
12 23 p r o v i s i o n i n g   c o d e   v a l u e
0C 17 70 72 6F 76 69 73 69 6F 6E 69 6E 67 20 63 6F 64 65 20 76 61 6C 75 65
```

### For the Min Wait Interval field:

1. Convert the value to hexadecimal. Note: you need to convert the actual number, not the hexadecimal representation of it.

The BroadBand Forum (the body that defined the format of these options) specified that this field is always four bytes in length. So once you've converted the number, the result needs to be padded with zeroes until it's the correct length.

```
      500
00 00 01 F4
```

2. The number of bytes is fixed at four, so no counting is necessary

```
  4
04
```

3. Convert the option code (13) to hexadecimal (0x0D). Convert the number, not the ASCII representation.

```
13
0D
```

4. Concatenate the results from step 3, step 2 and step 1 (in that order).

```
13  4      500
0D 04 00 00 01 F4
```

## For the Retry Interval Multiplier

1. Convert the value to hexadecimal. Note: you need to convert the actual number, not the hexadecimal representation of it. This field is also specified by the BBF to always be four bytes in length. The converted value therefore needs to be padded to be four bytes in length.

The BBF specifies this value must fall in the range 1000 - 65535 (<https://www.broadband-forum.org/cwmp/tr-181-2-9-0.html>).

```
      4000
00 00 0F A0
```

2. The length is fixed at four bytes by the specification.

```
      4
00 00 00 04
```

3. Convert the option code (14) to hexadecimal (0x0E). Convert the number, not the ASCII representation.

```
14
0E
```

4. Concatenate the results from step 3, step 2 and step 1 (in that order).

```
14  4      4000
0E 04 00 00 0F A0
```

Step 2. Join all the option strings together

Take each of the strings calculated at step 4 for each of the options above and join them together. The order is not important.

```
11 30 h t t p / / 1 9 2 . 1 6 8 . 4 2 . 2 3 9 8 0 8 0 / a c s
12 23 p r o v i s i o n i n g c o d e v a l u e 13 4 500 14
4 4000

0B 1E 68 74 74 70 3A 2F 2F 31 39 32 2E 31 36 38 2E 34 32 2E 32 33 39 3A 38 30 38 30 2F 61 63 73
0C 17 70 72 6F 76 69 73 69 6F 6E 69 6E 67 20 63 6F 64 65 20 76 61 6C 75 65 0D 04 00 00 01 F4 0E
04 00 00 0F A0
```

Step 3. Count the number of bytes in the string above (69) and convert to hexadecimal (0x45).

***It is important to emphasise that you simply cannot total the lengths reckoned in the second step of each option string creation.***

Those values do not take into account the fact that the string that is being counted includes information not present in each of the individual option strings.

```
69
45
```

Step 4. Convert the vendor ID (3156) to hexadecimal (0x0DE9).

***This field then needs to be padded to become four bytes in length.***

```
3156
00 00 0D E9
```

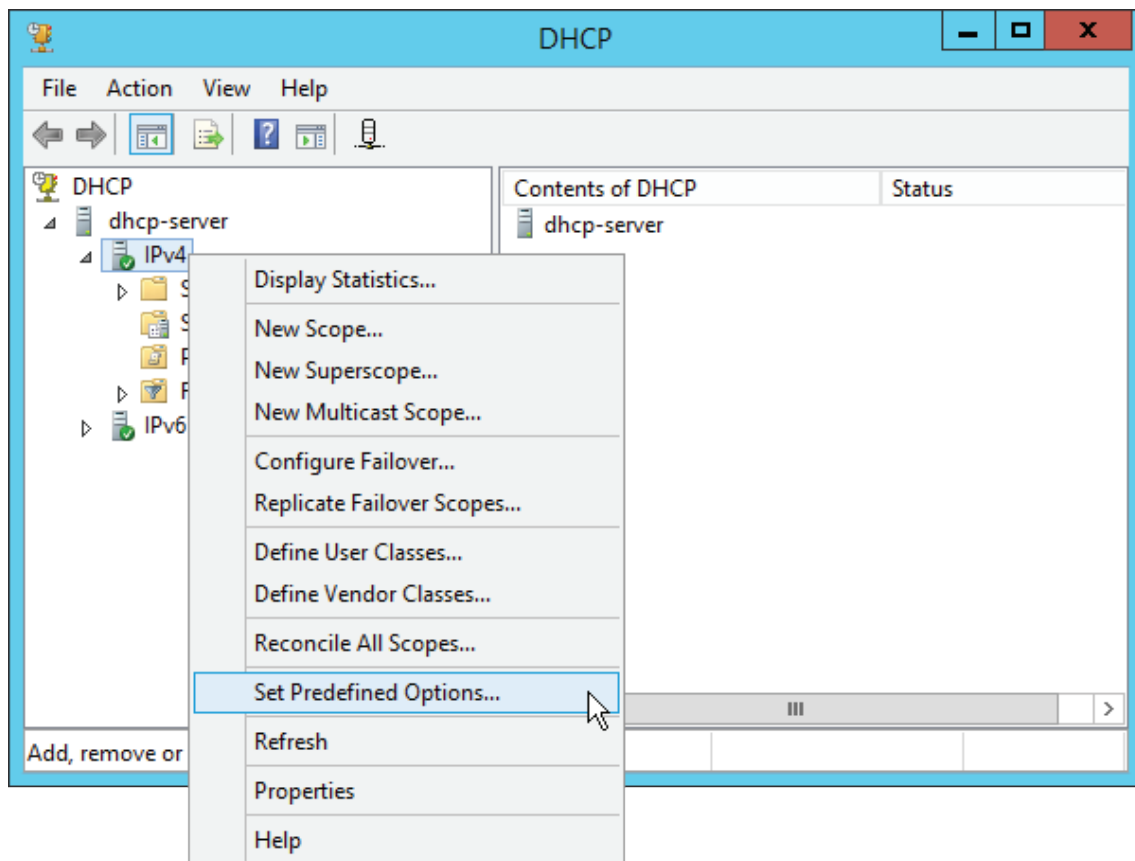
Step 5. Concatenate the strings in step 4, 3, and 2 above (in that order) to generate the finished string.

```
3156 64 11 30 h t t p / / 1 9 2 . 1 6 8 . 4 2 . 2 3 9 8 0 8
0 / a c s 12 23 p r o v i s i o n i n g c o d e v a l u e 13 4
500 14 4 4000

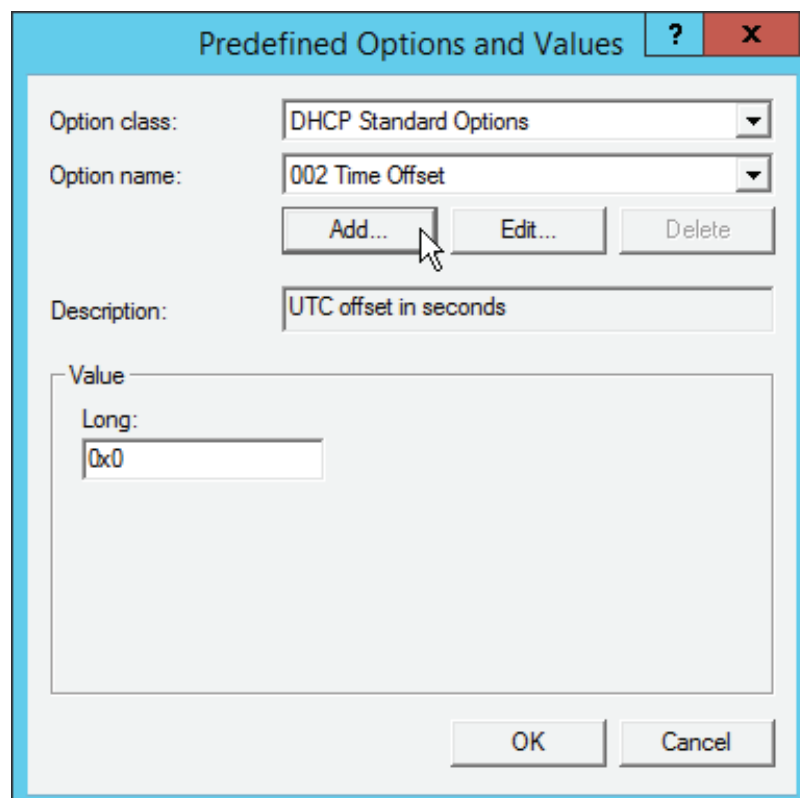
00 00 0D E9 45 0B 1E 68 74 74 70 3A 2F 2F 31 39 32 2E 31 36 38 2E 34 32 2E 32 33 39 3A 38 30 38
30 2F 61 63 73 0C 17 70 72 6F 76 69 73 69 6F 6E 69 6E 67 20 63 6F 64 65 20 76 61 6C 75 65 0D 04
00 00 01 F4 0E 04 00 00 0F A0
```

## Stage 2: Configuring Windows DHCP server

Step 1. Right click the "IPv4" server and select "Set Predefined Options".



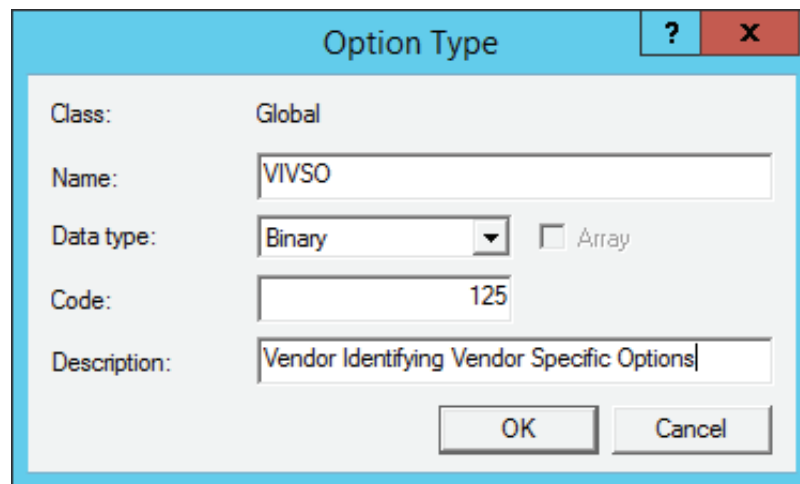
Step 2. The "Predefined Options and Values" window will appear. Click on "Add".



Step 3. Enter the following information into the "Option Type" window that appears:

Name: VIVSO  
Data type: Binary  
Code: 125

Click "OK" when done.

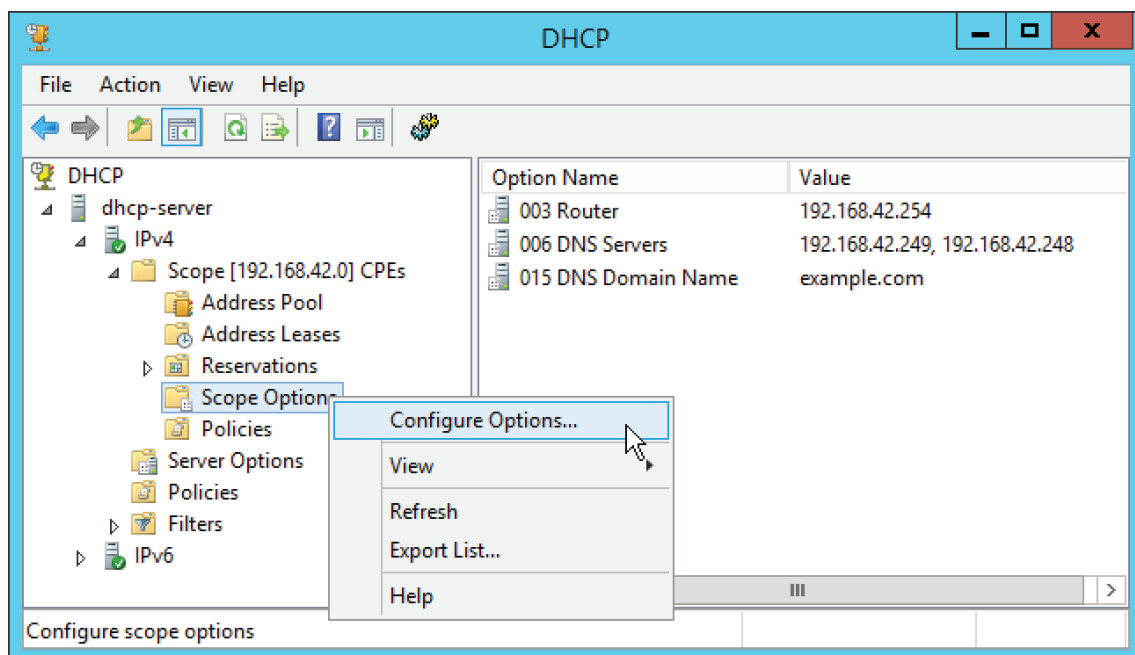


The "Option Type" dialog box is shown with the following fields:

- Class: Global
- Name: VIVSO
- Data type: Binary (selected from a dropdown menu, with an unchecked "Array" checkbox next to it)
- Code: 125
- Description: Vendor Identifying Vendor Specific Options

Buttons: OK, Cancel

Step 4. Back in the DHCP window, right click "Scope Options" and choose "Configure Options".

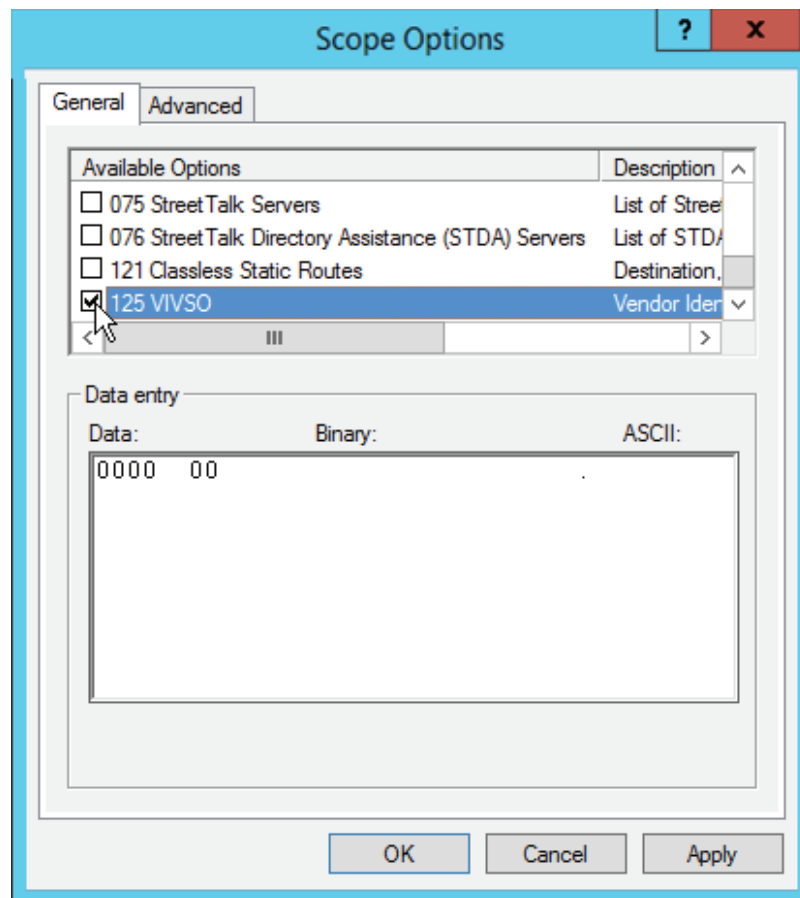




Step 5. Scroll down until you see option 125. Tick it.

By default, Windows pre-populates the option with a single 0x00 value. It is strongly recommended that you delete that value before entering the string calculated in stage 1. By failing to delete it, you run the risk of having a superfluous 0x00 in the final string which will cause the DHCP server to hand out invalid information.

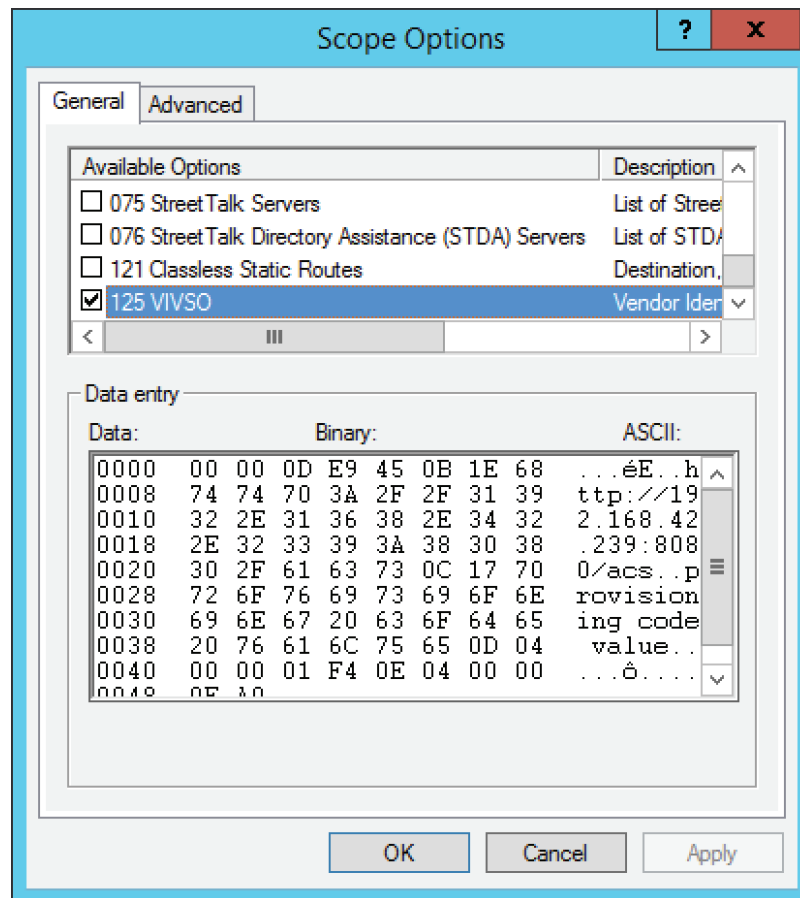
To delete the 0x00, place the cursor near the 0x00 in the "Binary" column and back space.



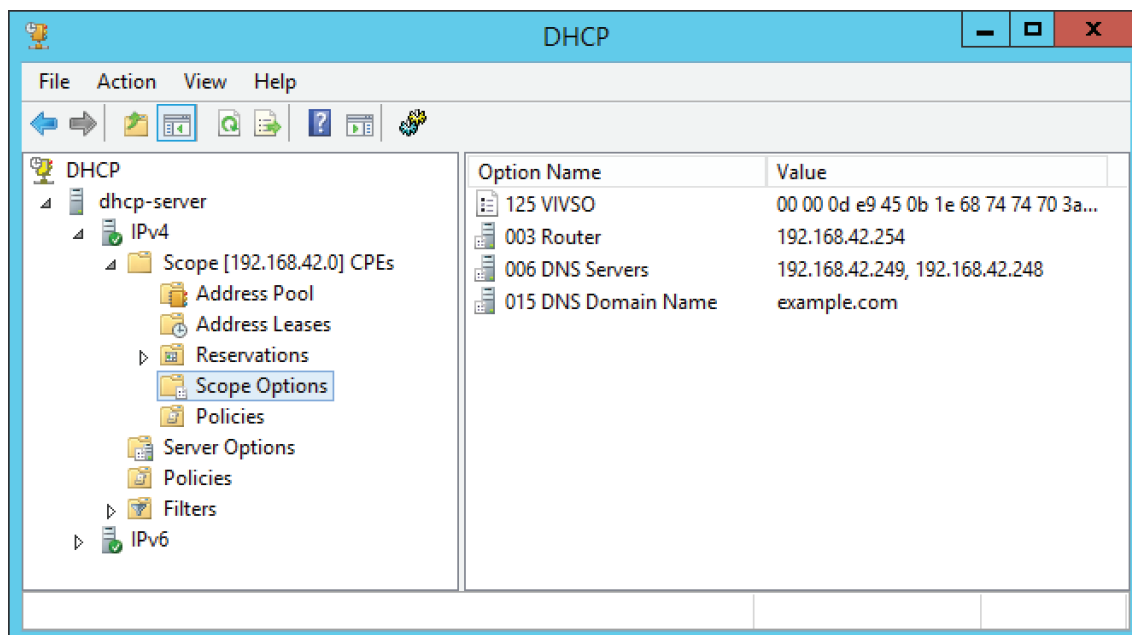
Step 6. With your cursor in the empty "Binary" column type in the hexadecimal string calculated in stage 1.

It does not appear to be possible to copy and paste the value, so care must be taken when typing the values in!

When finished, click "Apply".



You'll now see the option appear in the list with all the other configured options.



## Troubleshooting



**Note:** You cannot simply copy and paste these examples and change the option values. You need to perform all steps as detailed in this document in order to calculate the length values that will be unique to your settings.

To test option 125 has been configured correctly, use the CLI interface of the CPE to run debugging commands such as:

```
show running-config
show ccmp status
show dhcp client lease
```

## Appendix C. Glossary

---

Terminology	Definition
ACS	Auto Configuration Server. Used with the CWMP protocol.
CLI	Command Line Interface.
CPE	Customer Premises Equipment.
CWMP	CPE WAN Management Protocol.
DHCP	Dynamic Host Control Protocol
NTP	Network Time Protocol. Used to automatically configure the CPE with the correct time.
RPC	Remote Procedure Call
SSH	Secure Shell

GENEXIS



ALWAYS CONNECTED